This report was prepared by RAND, the Federal Bureau of Investigation's Criminal Justice Information Services Division, and the Bureau of Justice Statistics using federal funding provided by the Bureau of Justice Statistics.

Document Title: Comparison of Criminal-History Information Systems in the United States and Other Countries

Authors: RAND
Federal Bureau of Investigation, Criminal Justice Information Services Division
Bureau of Justice Statistics

Document No.: 253816

Publication Date: April 2, 2020

Award No.: This project was supported by award number 2016-R2-CX-K037.

Abstract:

Official criminal-history record information is an important component of criminal justice systems worldwide, but little is known about how the United States' criminal-history system compares to those in other industrialized countries. To address this knowledge gap, the Bureau of Justice Statistics sponsored a study to document and compare the national criminal-history systems in the United States, Australia, Canada, England and Wales, Germany, and the Netherlands. The topics include the operational uses and sources of the criminal-history data, procedures to assess record accuracy and completeness, efforts to improve the systems, and the availability of records to government and non-government entities for operational and research purposes. Sub-national criminal-history systems (e.g., the state repositories in the U.S.) and other data systems that maintain and disseminate criminal justice information were outside the scope of this study.

This page is intentionally left blank.

Comparison of Criminal-History Information Systems in the United States and Other Countries

RAND

Federal Bureau of Investigation, Criminal Justice Information Services Division

Bureau of Justice Statistics

Bureau of Justice Statistics

810 Seventh Street, NW

Washington, DC 20531

Acknowledgment

This report compares criminal-history information systems in the United States, Australia, Canada, England and Wales, Germany, and the Netherlands. The report discusses operational uses and sources of the criminal-history data, procedures to assess record accuracy and completeness, efforts to improve the systems, and availability of records to government and non-government entities for operational and research purposes.

The first chapter focuses on the national criminal-history system in the U.S. Section 1 of this chapter, on the criminal justice system, was produced by Mariel Alper of the Bureau of Justice Statistics (BJS). Sections 2, 3, and 4—on the national criminal-history record system, assessing criminal-history data quality and completeness, and accessing criminal-history data for research purposes—were produced by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services Division. Section 5, on using criminal-history data for research, was produced by Matthew Durose of BJS.

The U.S. chapter is followed by chapters, produced by RAND, on the national criminal-history systems in Australia, Canada, England and Wales, Germany, and the Netherlands. In consultation with the FBI and BJS, RAND also produced the last chapter, which compares the U.S. criminal-history system to the systems in the other countries.

Table of Contents

Key Findings**:**

- The United States consists of the federal government, 50 states, 5 permanently inhabited territories, and the District of Columbia. Each state maintains a criminal justice system under the state's unique laws, while also being subject to the federal criminal justice system.
- The Federal Bureau of Investigation (FBI) maintains the Next Generation Identification (NGI) System, which provides an automated biometric identification and criminal-history record (CHR) reporting system to support law enforcement agencies, criminal justice agencies, national security clearances, and authorized non-criminal-justice entities that conduct background checks on persons for non-criminal-justice purposes, such as employment and licensing.
- The NGI System is an identity-based, person-centric system that combines criminal and civil repositories. It includes records of fingerprints and in some cases palmprints; CHRs; mug shots; scar, mark, and tattoo photos; physical characteristics; and aliases.
- The Interstate Identification Index (III) is part of the NGI System and enables CHR data-sharing and integration across the U.S. The III is an index pointer system that ties the FBI's computerized CHR files and each III-participating state's centralized files into a national system. CHRs can include criminal justice information from police, prosecutor offices, courts, and correctional agencies.
- Criminal-history record information (CHRI) is made available for criminal justice, non-criminal-justice, and personal review purposes.
- Authorized criminal justice and non-criminal-justice agencies may access CHRs through an online III request or via a fingerprint submission to the NGI System.
- The FBI's Criminal Justice Information Services (CJIS) Division manages and maintains the NGI System and the III Program. The CJIS Division collaborates with federal, state, territorial, tribal, and local agencies to meet the needs of both the criminal justice and non-criminal-justice communities and to share responsibility for these programs.
- There are several restrictions on accessing and disseminating CHRI under federal laws and regulations.
- CHRI is voluntarily submitted by federal, state, territorial, tribal, and local agencies. Two areas of CHR improvement are missing dispositions and rap-sheet standardization.
- The use of CHR data for research requires review and approval from a governing Institutional Review Board.

US 1. Overview of the Criminal Justice System

The United States Constitution creates a system of government where power is shared between the federal and state governments. This system of federalism results in criminal justice operations organized at the federal and state levels.[1]

Law Enforcement

In the U.S., law enforcement agencies are responsible for enforcing laws and maintaining public order and public safety. Those responsibilities include preventing, detecting, and investigating crime and apprehending and detaining persons suspected of violating a law.[2] After an arrest, charges against the arrestee can be referred for prosecution or dismissed.

As of 2016, there are 86 federal law enforcement agencies with arrest and firearm authority, excluding intelligence and military organizations. Forty-three of these agencies are Inspectors General Offices that investigate criminal violations and prevent and detect fraud, waste, and abuse related to federal programs, operations, and employees. The majority of federal officers with arrest and firearm authority are in the U.S. Department of Homeland Security (DHS) or the U.S. Department of Justice (DOJ). The federal law enforcement agencies with the most full-time law enforcement officers authorized to make arrests and carry firearms are U.S. Customs and Border Protection and U.S. Immigration Customs Enforcement (both part of the DHS) and the Federal Bureau of Prisons (BOP) and the Federal Bureau of Investigation (FBI) (both part of the DOJ). The most common duties performed by federal law enforcement officers are criminal investigation and enforcement duties, corrections, police response and patrol, non-criminal investigation or enforcement, court operations, and security or protection.[3]

Of the 151,000 arrests by federal agencies in fiscal year (FY) 2016, 45% were for immigration offenses, 16% were for drug offenses, and another 16% were for violations of conditions of supervision.[4] Supervision violations include failures to appear in court and violations of bail, probation, and post-incarceration supervision. Two percent of arrests were for violent offenses.

In addition to federal agencies, there are about 15,000 general-purpose law enforcement agencies at the municipal, county, region, or state level as of 2016.[5] These agencies employ an estimated 701,000 full-time sworn law enforcement officers (who carry a firearm and a badge and have full arrest powers) and more than 349,000 full-time non-sworn employees. Local police departments employ 67% (468,000) of these full-time sworn officers.[6] Many of these local agencies are small, with about half employing fewer than 10 officers in 2016. Forty-five of these local agencies each employ more than 1,000 officers.

The law enforcement agencies include more than 3,000 sheriffs' offices employing about 173,000 full-time sworn officers in 2016.[7] Sheriffs' offices are typically organized at the county level and led by a sheriff who is elected. Like other law enforcement agencies, sheriffs' offices perform a range of law

[1] http://www.uscourts.gov/about-federal-courts/court-role-and-structure/comparing-federal-state-courts.
[2] https://www.bjs.gov/index.cfm?ty=tp&tid=7.
[3] *Federal Law Enforcement Officers, 2016 – Statistical Tables*, https://www.bjs.gov/content/pub/pdf/fleo16st.pdf.
[4] *Federal Justice Statistics, 2015-2016*, https://www.bjs.gov/content/pub/pdf/fjs1516.pdf.
[5] *Full-Time Employees in Law Enforcement Agencies, 1997-2016*, https://www.bjs.gov/content/pub/pdf/ftelea9716.pdf.
[6] *Local Police Departments, 2016: Personnel*, https://www.bjs.gov/content/pub/pdf/lpd16p.pdf.
[7] *Sheriffs' Offices, 2016: Personnel*, https://www.bjs.gov/content/pub/pdf/so16p.pdf.

enforcement functions, including responding to criminal incidents and calls for service. However, unlike other agencies, sheriffs' offices also typically operate local jails and provide services to criminal courts, such as courthouse security.

Law enforcement agencies nationwide made almost 10.7 million arrests in 2016, including almost 12,000 arrests for murder or non-negligent manslaughter, almost 1.6 million arrests for drug abuse violations, more than 1 million arrests for driving under the influence, and more than 1 million arrests for larceny or theft.[8]

Courts

Historically, federal courts have prosecuted crimes defined by federal law and the Constitution. However, the role of federal courts in criminal prosecution grew as federal penalties were established for crimes that had traditionally been prosecuted in state courts. Beginning in the second half of the twentieth century, new statutes made federal crimes of murder, kidnapping, theft, bank robbery, extortion, and possession of illegal firearms when they involved crossing state lines or the use of facilities of interstate commerce. Laws also established federal jurisdiction over crimes that affected interstate commerce in some way, including actions related to civil rights, drugs, gambling, loan sharking, sexual abuse, and violence against minority groups.[9]

In FY 2016, federal district courts disposed of almost 77,000 cases involving a violation of a federal law through a guilty plea, bench or jury trial, or dismissal. Almost 53,000 defendants were detained while awaiting trial in a federal court.[10] The largest percentage of cases disposed by federal courts were for immigration offenses (more than 45% of cases), followed by drug offenses (more than 20%).

As of 2011, there were more than 27,000 trial court judges, nearly 1,000 appellate court judges, and more than 300 judges in courts of last resort.[11] Elections are a common way to select judges for their initial term, with 48% of appellate judges and 75% of trial judges selected this way. Judges who are not elected are appointed. Depending on the state, appointments may be made by the governor, legislature, or chief justice. Among elected judges, some run in a contested election in which candidates must declare their political party affiliation (partisan election) and some run in a contested election in which they do not declare a political party affiliation (non-partisan election). For subsequent terms, some sitting judges retain their office through an uncontested retention election whereby they maintain their position if the majority votes that they should be retained in office.

[8] https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/tables/table-18.
[9] https://www.fjc.gov/history/courts/jurisdiction-criminal.
[10] *Federal Justice Statistics, 2015-2016*, https://www.bjs.gov/content/pub/pdf/fjs1516.pdf.
[11] *State Court Organization, 2011*, https://www.bjs.gov/content/pub/pdf/sco11.pdf.

Corrections

There were more than 6.6 million persons (or about 1 in 38 adults) under the supervision of adult correctional systems in the U.S. on December 31, 2016. [12] In most jurisdictions, adults are persons age 18 or older. At the end of 2016, there were more than 1.5 million adults in prison, more than 700,000 in local jails, almost 900,000 on parole, and almost 3.7 million on probation.

Some persons age 17 or younger may be prosecuted in the adult criminal justice system and considered adults. Other persons age 17 or younger are under the jurisdiction of a juvenile court or agency. Adults may be incarcerated in a prison or jail. Prisons are run by the state or federal government and typically hold felons and offenders with a sentence of more than one year, although this cutoff varies by jurisdiction. Jails are usually administered by a local law enforcement agency for confinement before and after adjudication. Jail inmates who have been adjudicated usually have a sentence of one year or less.

Adults may also be under supervision in the community, either under parole or probation. Parole is a conditional release to the community after a prison term. During this supervision period, parolees are under the supervision, control, or care of a state or federal correctional agency. Violations of conditions of community supervision may result in a new confinement sentence or a return to confinement for a technical violation of release conditions. Persons may be released from state or federal prison to parole through discretionary decisions such as a parole board decision or a mandatory release that is determined by law. The availability of these release mechanisms varies by jurisdiction.

Probation is a court-ordered period in the community under the supervision, control, or care of a correctional agency, usually at the state or local level. Probation is a contract with the court in which the person must abide by the probation conditions to remain in the community. Though it is similar to parole in practice, probation is generally ordered instead of incarceration. Probation often entails monitoring and surveillance by a correctional agency, though in some cases probation may not involve any reporting requirements.

[12] *Correctional Populations in the United States, 2016*, https://www.bjs.gov/content/pub/pdf/cpus16.pdf.

US 2. Understanding the National Criminal-History Record System

The Federal Bureau of Investigation

Biometric identification, which includes the processing of fingerprint submissions and criminal-history records (CHRs), has long been the responsibility of the Federal Bureau of Investigation (FBI). Since 1921, the FBI has been authorized by law to collect and disseminate criminal-history record information (CHRI), which is defined as "information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system."[13]

After centralizing CHRs at the FBI, the need to improve the quality and organization of CHRs in the U.S. became apparent. These improvements and the nationwide consolidation of fingerprint files were delegated to the FBI. On July 1, 1924, the FBI established the Identification Division to gather fingerprints from law enforcement agencies nationwide and, upon request, search the fingerprints for matches to criminals and crime evidence.

On June 11, 1930, the FBI's statutory authority to collect and disseminate CHRI was codified at Title 5, United States Code (U.S.C.), Section 340, which was twice recodified as the current 28 U.S.C. § 534 to provide for the acquisition, preservation, and exchange of identification records and information by the U.S. Attorney General (AG). As amended, this authority empowers the FBI to exchange CHRI with, and for the official use of, "authorized officials of the Federal Government, including the United States Sentencing Commission, the States, including State sentencing commissions, Indian tribes, cities, and penal and other institutions."

Over time, the FBI's responsibilities expanded and new technology allowed for automated fingerprint processing and CHR reporting. In February 1992, the Identification Division merged with other FBI programs to form the Criminal Justice Information Services (CJIS) Division. The CJIS Division is the focal point and central repository for criminal justice information services in the FBI, including the national fingerprint identification and CHR system.

The Next Generation Identification System

In July 1999, the CJIS Division deployed the Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS provided automated fingerprint searches, electronic image storage, electronic exchanges of fingerprints and responses, and authorized text-based searches using descriptive information. Criminal and civil records were in separate repositories with no mechanism to search and link the records. Advances in technology necessitated further development of identification services. The CJIS Division, with guidance from the user community, developed the Next Generation Identification (NGI) System to meet the evolving business needs of IAFIS customers.

[13] Title 28, Code of Federal Regulations, Part 20.3 and 34 U.S.C. § 40316.

The FBI owns and operates the NGI System and deployed it in September 2014. It provides an automated biometric identification and CHR reporting system to support law enforcement agencies, criminal justice agencies, national security clearances, and authorized non-criminal-justice entities that conduct background checks of persons for employment or licensing purposes or persons serving in positions of trust. The NGI System is an identity-based, person-centric system that combines the criminal and civil repositories. Upon successful submission, each identity is linked to all retained criminal and civil biographic and biometric data via an FBI Universal Control Number (UCN). The UCN is a unique identifying number created by the FBI to establish civil and criminal identities or any combination thereof.

The records in the NGI System include fingerprints; palmprints; corresponding CHRs; mug shots; scar, mark, and tattoo photos; physical characteristics such as height, weight, hair color, and eye color; and aliases. As of 2016, the NGI System houses more than 72 million criminal fingerprints, more than 51 million facial images, and records for more than 700,000 registered sex offenders.[14] The NGI System also includes more than 50 million civil fingerprints for persons who served or are serving in the U.S. military or who were or are employed by the federal government, as well as civil fingerprints submitted by authorized state and federal agencies requesting FBI retention.[15]

Data in the NGI System is maintained according to retention schedules approved by the National Archives and Records Administration (NARA). The NARA approved the destruction of fingerprint cards and corresponding indices when criminal and civil subjects reach age 110.[16] Biometric and associated biographic information may be removed from the NGI System earlier than the standard NARA retention period via a request from the agency that contributed the information or via court order. All fingerprints and CHRI maintained in the NGI System are submitted voluntarily by federal, state, territorial, and tribal agencies.

Although the FBI has migrated to an automated identity management structure that maintains all information about a person in a single record based on a unique identity, the criminal and civil files remain logically separated. The NGI System's logical dissemination rules enable the NGI System to disseminate a CHR based on the purpose of the search and the CHRI the user is permitted to receive, as authorized by a federal or state law.

The Interstate Identification Index

The Interstate Identification Index (III) is part of the NGI System and enables CHR data-sharing and integration across the country. The III is an index pointer system that ties computerized CHR files of the FBI and the centralized files maintained by each III-participating state into a national system. When the III Program began in 1983, III-participating states became accountable for responding to online queries for state-maintained CHRs for all purposes the state could legally support. Today, 51 State Identification Bureaus (SIBs), including the District of Columbia, participate in the III Program.

---

[14] *FBI CJIS Division 2016 Annual Report*, https://www.fbi.gov/file-repository/2016-cjis-annual-report.pdf/view.
[15] *Ibid.*
[16] *NGI Retention and Searching of Noncriminal Justice Fingerprint Submissions*, https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

III-participating states establish and update records within the III through the submission of fingerprint images from first and subsequent arrests to the NGI System. Each CHR maintained within the III is supported by a fingerprint submission and is assigned a unique UCN. However, unlike the NGI System, which contains biometric data, the III includes only names and personal identification information relating to persons who have been arrested or indicted for a serious criminal offense anywhere in the country. The III includes persons born in 1956 or later for whom an arrest fingerprint card has been submitted to the FBI at any time; persons born prior to 1956 whose first arrest fingerprint card was submitted to the FBI on or after July 1, 1974; numerous older records; certain fugitives; and repeat offenders. The FBI maintains these individuals' automated fingerprints and automated CHRs, which originate from more than 17,000 arresting agencies in the U.S.

The III provides a means of conducting national CHR searches for criminal justice and other authorized purposes as specified by existing statutory authority. The III Program is built on duplicate CHR repositories and shared record dissemination between the III and state systems. Once the state adds the fingerprint submission and arrest data to its state repository, the state sends a duplicate to the NGI System for inclusion in the national database. The FBI maintains the duplicate records, including records the III states cannot support, and the federal arrest information. The FBI uses the duplicate records to respond to online queries and fingerprint processing record requests for any purpose for which a state cannot respond. An authorized criminal or non-criminal-justice agency may access CHRs through an online III request or via a fingerprint submission to the NGI System.

Online Queries

The III enables online name-based queries and record requests using biographic descriptors, a State Identification Number (SID),[17] a UCN, or any combination thereof, to review a CHR or to determine whether there is a matching index record on file. When the III receives an online record request supported by a III-participating state, the III automatically sends a message to the state's computer system. The state responds directly to the requesting agency. The FBI responds for records for federal offenders; for persons arrested in non-III states and U.S. territories; and for criminal arrests that the III states cannot support. For example, if a person is arrested in State A and has CHRI from State B and State C, then depending on the query's purpose, the III will reach out directly to State B and State C, using either the UCN or the SID, to obtain the CHRI from each state **(figure 1)**.

[17] A SID is a unique number assigned to a person by the state.

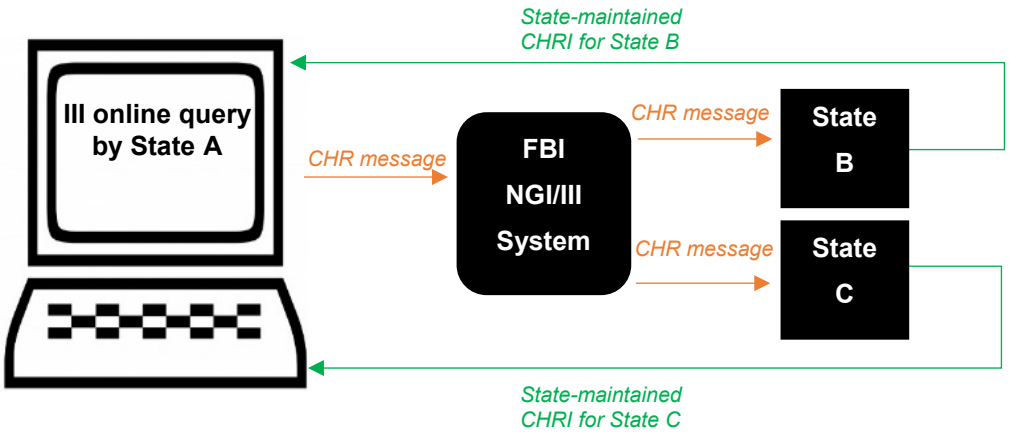


Figure 1

When a state cannot respond with its CHRI, the FBI will provide what it has on file for that particular state. For example, if the same individual arrested in State A applies for employment requiring an FBI fingerprint-based background check and has CHRI from State B and State C, the FBI will provide the information in its database for State C if State C does not respond to requests for CHRI for employment and licensing purposes **(figure 2)**.

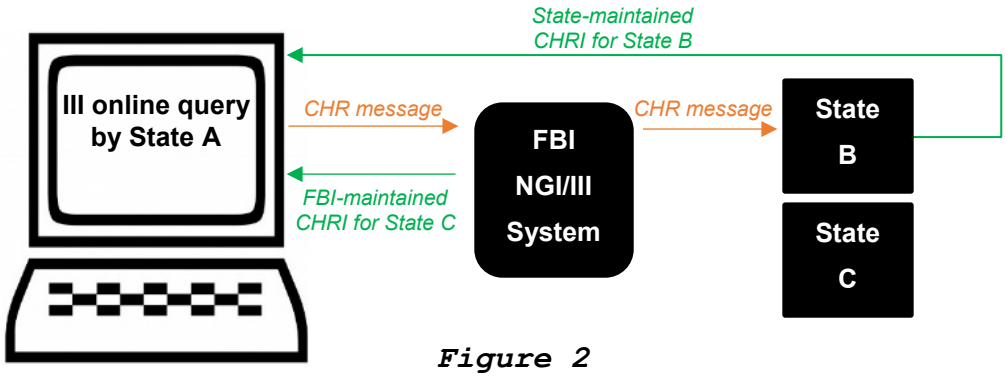


Figure 2

States may not be able to respond to CHR requests due to varying laws and regulations. Moreover, if the FBI does not have all relevant information from the state when responding on its behalf, any additional state-maintained information will not be available for dissemination.

Fingerprint Submission

An authorized agency may receive CHRI by submitting fingerprints to the FBI to search the NGI System. Each CHR is supported by a criminal fingerprint submission, which is acquired as a result of an arrest at the federal, state, territorial, tribal, or local level. For persons arrested in states or U.S. territories, the arresting agency submits the fingerprint images to the SIB for processing and assignment of a SID. The SIB updates its state file and voluntarily sends the arrest information to the FBI's NGI System. If no prior record is on file, the FBI establishes a new record and assigns a UCN. The submitting agency receives a

response stating no record exists at the national level, while the fingerprint images, along with the name and descriptive information (sex, race, date of birth, Social Security number, and aliases) appearing on the fingerprint submission, are retained as part of the CHR. It is then the submitting agency's responsibility to forward any information, such as dispositions, for addition to the CHR on file at the FBI. If subsequent fingerprint images are sent to the FBI for the newly created identity, the NGI System will return a positive identification response to the submitting agency, including the UCN and a copy of the CHR. The same is true for federal agencies that submit directly to the FBI **(figure 3)**.

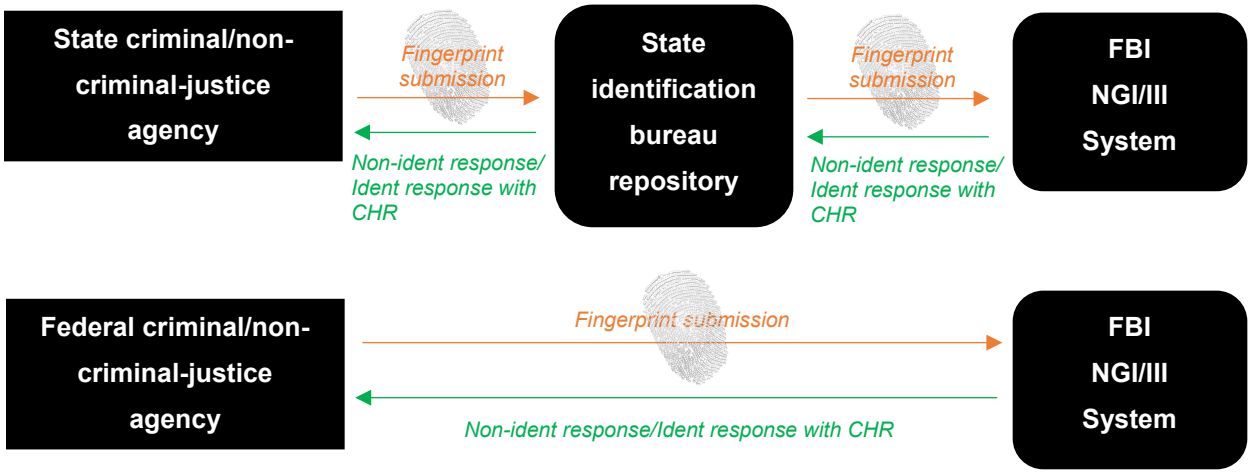


Figure 3

To provide the most up-to-date CHRI, once a fingerprint submission is identified to a UCN at the national level, the NGI System uses the III "pointers" to determine whether a state or the FBI is responsible for maintaining and disseminating the various parts of a person's CHR. Like online queries, the pointer is used to direct searches of records to the appropriate agency. A state-active pointer is indicated by a SID and directs the search to the state central repository if the state's policy supports disseminating information for the purpose for which fingerprints were submitted. The NGI System follows the III pointer and automatically sends a message to the state that holds the record and appends the state record to the NGI System's response. The state information stored within the NGI System identified with the pointer is suppressed from the response to reduce the risk of duplication. If the state does not support the purpose of the fingerprint search, the FBI will not send a message to the state and will respond with any information in its database for that particular state. When the FBI controls the dissemination of a state or federal record, the record is indexed in the III with a pseudo-pointer. The FBI is responsible for disseminating records indexed in the III with a pseudo-pointer.

For example, if a fingerprint submission is identified to a record with CHRI from State A (active state pointer) and State B (pseudo-pointer), using State A's SID, the FBI will send a message to State A to obtain the state-maintained CHRI. If State A responds for the purpose of the request, the FBI will not return any CHRI maintained in the FBI database for State A. Instead, the FBI will append the information provided by State A in the final response to the contributing agency. The FBI will also respond with any information in its database for State B because State B is indexed as a pseudo-pointer **(figure 4)**.

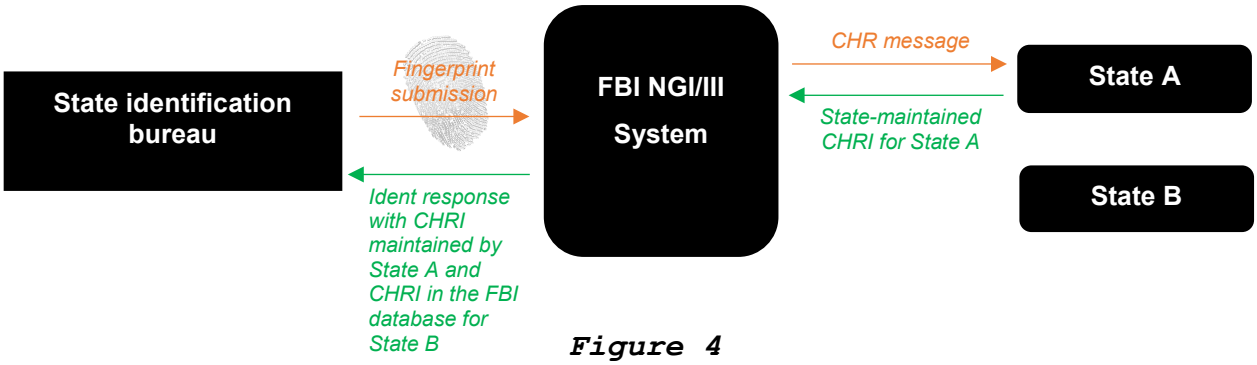


Figure 4

In addition to criminal fingerprints and CHRs, the NGI System includes civil fingerprints. A contributing agency must be authorized to submit the civil fingerprints to the NGI System and receive the FBI CHRI. The FBI may retain fingerprints of a person who is subject to an FBI background check for employment or licensing purposes at the contributing agency's request. Any person whose fingerprints are submitted to the FBI for non-criminal-justice purposes must be provided a Privacy Act Statement regarding the retention and search of their fingerprints in the NGI System. Civil fingerprint submissions received and retained by the FBI are stored electronically within the NGI System and receive a UCN to establish an identity at the national level if no identity currently exists. If the contributing agency requests removal of the civil fingerprints, or removal is required by court order, the retained civil fingerprints will be removed from the NGI System.

National Fingerprint File Program

The final phase of III implementation is decentralization, in which the FBI compiles a national CHR from participating state repositories. The National Fingerprint File (NFF) Program replaces the FBI's record-keeping responsibility for state offenders by making state repositories primarily responsible for the effective control, collection, maintenance, and dissemination of state CHR files. To become an NFF participant, a state must meet certain requirements, including ratification of the National Crime Prevention and Privacy Compact Act of 1998 (Compact). An NFF-participating state is a III-participating state that has agreed to provide its CHRs for all authorized uses, including non-criminal-justice licensing and employment purposes.

The process for submitting fingerprints is different for states participating in the NFF Program. An NFF-participating state submits fingerprint images to the FBI for each offender's first arrest to identify the offender at the national level. Fingerprint images for subsequent arrests are used by the state to update its own records. Only those criminal fingerprint images that a state is unable to identify will be forwarded to the NGI System. Any subsequent activity related to the NFF record will be the NFF-participating state's sole responsibility. The NFF-participating state does not submit supporting documentation to the NGI System such as subsequent arrest information, expungement requests, disposition reports, and death notices. As a result, the NFF-participating states must meet certain NFF qualification requirements to ensure proper NFF participation.

If an online query or a fingerprint-based submission identifies a person with a CHR in one or more NFF-participating states, a request for the CHR will be forwarded from the NGI System to the NFF-participating state's CHR repository for the appropriate response. The NFF-participating state provides its CHR to the NGI System to be appended to the FBI's response and disseminated to the contributing agency. Currently, 20 states participate in the NFF Program.[18]

CHRI Maintenance

State agencies participating in the III Program must—

1. ensure each record contains all known arrest, disposition, and custody or supervision data for the state
2. remove or expunge a SID from a III record when the corresponding record data no longer exists at the state level
3. conduct a regularly scheduled audit to identify discrepancies and synchronize the III records pointing to the state's database
4. maintain records at the highest possible level of completeness, accuracy, and timeliness.

For the FBI to provide the most accurate records to requesting agencies and entities, all CHRI must be available, accurate, and complete. Under 28 C.F.R. § 20.37—

> It shall be the responsibility of each criminal justice agency contributing data to the III System … to assure that information on individuals is kept complete, accurate, and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred.

For the FBI to disseminate the most complete and accurate CHRs for the NGI System fingerprint submissions and the III inquiries, all necessary corresponding information pertaining to an arrest must be provided to the FBI. The FBI CJIS Division processes requests associated with CHRs received in electronic, hard-copy, or machine-readable data formats. These documents include arrest dispositions, custody data, expungements, and other miscellaneous updates.

Dispositions

In every instance when criminal arrest fingerprints have been submitted to the FBI prior to disposition, the final disposition must be submitted to update the CHR. A disposition is the formal or informal conclusion of an arrest or charge at whatever stage it occurs in the criminal justice system. A disposition reports the court's findings and can include information as to whether an arrest charge has been modified or dropped.[19] A more inclusive definition of a disposition is located at 28 C.F.R. § 20.3.

[18] For the most recent list of NFF-participating states, visit https://www.fbi.gov/services/cjis/compact-council/interstate-identification-index-iii-national-fingerprint-file-nff.
[19] *Arrest Disposition Submission,* https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/arrest-disposition-submission.

Disposition reporting is important to law enforcement for investigative purposes and to non-criminal-justice background checks for employment, licensing, adoption, and immigration. If a disposition is not in the person's CHR, it could prevent or delay the adjudication for these proceedings. As such, the III and the FBI CJIS Division offer various electronic methods for states to add disposition data to the CHR, such as the III messaging or fingerprint submission. States may also send hard-copy dispositions to the FBI for manual processing.

Custody and Supervision Data

A state or agency may update the CHR by submitting custody and supervision requests to the FBI CJIS Division in electronic or hard-copy formats. The custody and supervisory data is posted to a CHR, including information pertaining to supervised or mandatory release and parole, probation, or pretrial diversion. Under pretrial diversion, the arrest is removed from the CHR if the subject completes supervision and abstains from criminal activity for 3 years.

Expungements

An expungement is the removal of CHRI. As such, states may choose to expunge the entire CHR or part of the CHR (e.g., one of the charges associated with an arrest) by sending the appropriate electronic message via the III. If the state cannot generate a III message, the FBI CJIS Division can do expungements on the state's behalf, based on receipt of necessary expungement documentation. The FBI CJIS Division can also perform expungements at the request of federal, territorial, or tribal agencies.

Biographic Identifiers

Although most biographic identifiers (e.g., aliases or additional dates of birth) are entered into the III as a result of a fingerprint submission, an agency may have documentation that is not provided to the FBI that contains new identifiers. States may add identifiers to the III by sending the appropriate III message to update the CHR. States also have the ability to remove or correct biographic identifiers on a CHR, so long as the identifier was added to the CHR by the requesting state. Those agencies unable to add or remove biographic identifiers via the III may submit the appropriate form to the FBI CJIS Division for handling.

National Sex Offender Registry

In July 1999, the National Sex Offender Registry (NSOR), then known as the Convicted Sex Offender Registry File, was established within the National Crime Information Center (NCIC). The NSOR contains records of sex offenders or other persons required to register under a jurisdiction's sex offender registry program. When registering an offender, the authorized state criminal justice agency includes the information in the state sex offender registry and the NSOR via an online record entry. Authorized federal and tribal criminal justice agencies may also maintain agency-specific sex offender registries and contribute records to the NCIC NSOR. If the NSOR record contains a UCN, the NCIC notifies the NGI System. This notification causes the NGI System to establish a sex offender notice on the person's CHR. This notice will then appear on CHRs in response to both III inquiries and fingerprint submissions.

Agencies must submit complete and accurate information for convicted sex offenders to the NCIC NSOR, including the UCN, if known. If the UCN is not included upon entry in the NCIC NSOR, the person's CHR will not be flagged with a sex offender notice in the NGI System. Agencies that cannot determine or verify an offender's UCN can submit fingerprints to the NGI System as a criminal inquiry to conduct a search, verify the identity of the person, and obtain the UCN for inclusion in the NCIC NSOR and subsequently the CHR.

Shared Management Responsibilities

The mission of the FBI CJIS Division is to equip its law enforcement, national security, and intelligence community partners with criminal justice information needed to protect the U.S. while preserving civil liberties. As the central repository for criminal justice information and services within the FBI, the CJIS Division manages and maintains several systems, such as the NGI System and the III Program, which are used by the division's federal, state, territorial, tribal, and local partners. The CJIS Division collaborates with federal, state, territorial, tribal, and local agencies to meet the needs of both the criminal justice and non-criminal-justice communities.

Advisory Policy Board

The FBI established the CJIS Advisory Process[20] to obtain users' advice and guidance on the development and operation of all CJIS Division programs. The CJIS Advisory Policy Board (APB) includes representatives from criminal justice agencies, national security agencies, and criminal justice professional associations across the U.S. Twice each year, the APB makes recommendations to the FBI director regarding general policy with respect to the philosophy, concept, and operational principles of these criminal justice information systems. If the FBI director approves the CJIS APB recommendation, the staff from the FBI CJIS Division takes the necessary action to implement the change.

The National Crime Prevention and Privacy Compact Council

The Compact, as codified at 34 U.S.C. § 40316 (formerly cited as 42 U.S.C. § 14616), provides a legal framework for the establishment of a cooperative federal-state system for the interstate exchange of CHRI for non-criminal-justice uses. Some states participating in the III Program have varying statutes or policies that restrict the dissemination of records for non-criminal-justice purposes. However, under the Compact, the Federal Government and states agree to make their respective CHRs available to parties of the Compact for authorized non-criminal-justice purposes. The Compact facilitates uniformity in the dissemination of records among states for non-criminal-justice purposes and requires that a signatory state provide its records upon request for all authorized non-criminal-justice purposes. As mentioned, a state must ratify the Compact prior to joining the NFF Program. As more states ratify the Compact and participate in the NFF Program, non-criminal-justice data will be shared in a more uniform and decentralized way. Thirty-four states have ratified the Compact as of July 2019, and 20 of those states participate in the NFF Program.[21]

[20] For additional information regarding the CJIS Advisory Process, visit https://www.fbi.gov/services/cjis/the-cjis-advisory-process.
[21] For more information on the National Crime Prevention and Privacy Compact Act of 1998, visit https://www.fbi.gov/services/cjis/compact-council.

The Compact also established a 15-member Council. Its mission as a national independent authority is to enhance public safety through non-criminal-justice background checks based on positive identification, while protecting individual privacy rights. The Council oversees the use of the III, promulgates rules and procedures for the effective and proper use of the III for non-criminal-justice purposes, ensures the protection of privacy, and facilitates the nationwide exchange of CHRI.

Access to CHRI

The FBI must maintain an audit trail of the recipient of each record and of the purpose of each disclosure of a CHR. To ensure the transaction is authorized, each III inquiry must include the purpose for which the subject's record information will be used. Fingerprint-based applicant submissions must include the "reason fingerprinted" to indicate the authority under which the CHRI will be used. All users are required to provide the reason for all III inquiries and fingerprint-based transactions upon request by CJIS systems managers, administrators, and representatives. In addition, agencies are aware that access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

When appropriate, prior to accessing the CJIS record information systems, each federal, state, territorial, or tribal agency must execute a CJIS User Agreement with the FBI CJIS Division stating its willingness to conform with federal statutes, regulations, and CJIS policies. These agreements include the standards and sanctions governing the use of the CJIS systems. Once the established qualifying criteria are met and access to CJIS systems is approved, agencies are assigned and receive an Originating Agency Identifier (ORI). The ORI structure determines the type of access and allows the agency to use various CJIS systems, such as the NGI System. Access to CHRI is made available for criminal justice, non-criminal-justice, and personal review purposes.

Criminal Justice Purpose

An individual's CHR may be disseminated to criminal justice agencies for criminal justice purposes, which include the screening of employees or applicants for employment hired by criminal justice agencies.[22] A criminal justice agency is defined as (1) the courts; or (2) a governmental agency, or any subunit of a governmental agency that performs the administration of criminal justice pursuant to a statute or executive order and that allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.[23]

Administration of criminal justice is defined at 28 C.F.R. § 20.3(b) as follows:

> Administration of criminal justice means performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The

[22] 28 C.F.R. § 20.33(a)(1).
[23] 28 C.F.R. § 20.3(g).

administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal-history record information.

The definitions of a "criminal justice agency" and the "administration of justice" must be considered together.[24]

Non-Criminal-Justice Purpose

An agency may access CHRI for non-criminal-justice purposes, such as employment or licensing, only when authorized by federal statutory authority. For example, in 1971, Congress enacted P.L. 92-184, which was superseded in 1972 by P.L. 92-544 (34 U.S.C. § 41101). This statute authorized the exchange of FBI identification records with officials of federally chartered or insured banking institutions to maintain the security of those institutions, and with officials of state and local governments for licensing and employment purposes if authorized by a state statute the U.S. AG has approved. The AG's approval authority is delegated to the FBI by 28 C.F.R. §§ 0.85(j) and 50.12(a). The FBI uses specific criteria to approve state statutes enacted under P.L. 92-544 to ensure all requirements are met. The FBI policy requires that fingerprints submitted to the FBI under P.L. 92-544 state statutes be channeled through the SIB. A governmental agency, designated by statute, must be responsible for receiving and screening the results of the CHR check to determine an applicant's suitability for employment or licensing. Purposes in which CHRI is used for non-criminal-justice employment and licensing include teaching, nursing, and real estate.

In addition to state statutes, numerous federal statutes, as well as executive orders, exist to provide a means of conducting national CHR searches for non-criminal-justice purposes. Each authority defines the specific purpose (applicant types) for which CHRI may be requested and used. Some examples of federal statutes include the National Child Protection Act/Volunteers for Children Act; the Adam Walsh Child Protection and Safety Act of 2006; the Native American Housing Assistance and Self-Determination Act of 1996; and the Serve America Act. Prior to implementation of any federal statutory authority, a federal, state, territorial, or tribal agency must coordinate with the FBI to determine the requirements for submitting under the specific authority.

Pursuant to the Compact, all requests for background checks for non-criminal-justice purposes must be conducted based on positive identification. Currently, the only approved forms of positive identification are 10-flat or 10-rolled fingerprints.[25] Positive identification ensures the subject of the record search is the same person as the subject of the CHR.

Personal Review

Under 28 C.F.R. §§ 16.30-16.34, any individual may obtain a copy of his or her FBI CHR by submitting a Departmental Order (DO) 556-73 request, fingerprints, and the appropriate fee. The CHRs provided through the DO process may be used to challenge the information on the record. For individuals challenging a record, the FBI CJIS Division forwards the challenge to the agency that submitted the data

[24] 28 C.F.R. Part 20 Appendix.
[25] 70 Fed. Reg. 36209.

to request the agency verify or correct the challenged entry. While the FBI CJIS Division serves as the nation's central repository and custodian for fingerprints and CHRI, it does not have the authority to modify any CHRI unless specifically notified to do so by the contributing agency.

Dissemination of CHRI

The U.S. Code, federal regulations, and the National Crime Prevention and Privacy Compact provide safeguards against dissemination of CHRI. Title 28 U.S.C. § 534 authorizes the FBI to exchange CHRI with, and for the official use of, authorized officials of the federal government, the states, Indian tribes, cities, and penal and other institutions. The exchange of CHRI made available pursuant to this authority is subject to cancellation if dissemination is made outside the receiving departments or related agencies.

Title 28 C.F.R. § 20.33 further specifies that CHRI contained in the III may be available for use in connection with licensing and employment pursuant to P.L. 92-544 or other federal legislation or federal law. This regulation reiterates the requirement that the exchange of CHRI is subject to cancellation if dissemination is made outside the receiving departments or related agencies. It also stipulates that CHRI shall be used only for the purpose requested and a current record should be requested when needed for a subsequent authorized use.

Title 28 C.F.R. § 50.12 also sets forth requirements for the exchange of CHRI for non-criminal-justice purposes authorized by federal law to include P.L. 92-544. This regulation provides that CHRI obtained under these authorities may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities.

In addition, the Compact requires that any CHRI obtained under the Compact may be used only for the official purposes for which the CHRI was requested.[26] Further, the Compact established procedures to protect the accuracy and privacy of CHRI by requiring that CHRI must be used only by authorized officials for authorized purposes and that subsequent record checks be requested to obtain current information whenever a new need arises.

Moreover, CHRI must not be disseminated to the general public. The FBI CHRI may also not be maintained in a format that is accessible by the public or within records that are subject to release through public record requests.

National Rap Back Service

In 2014, the national Rap Back Service was created with the deployment of the NGI System. This service allows authorized federal, state, and local agencies to be notified of activity reported to the NGI System on persons who are licensed or employed (e.g., school teachers and day-care workers) or who are under criminal justice supervision or investigation, eliminating the need for repeated background checks on a person from the same agency.

[26] 34 U.S.C. § 40316.

Before the FBI's Rap Back Service, the national criminal-history background check system provided a one-time snapshot of a person's criminal-history status. With Rap Back, authorized criminal justice and non-criminal-justice agencies can receive ongoing notifications of any criminal activity reported to the FBI after the initial processing and retention of criminal or civil fingerprints. Rap Back accomplishes this by using fingerprints to identify persons arrested and prosecuted for crimes.

US 3. Addressing Criminal-History Data Quality and Completeness

The FBI is committed to supporting the criminal justice and the non-criminal-justice communities, intelligence agencies, and the public by improving processes and standards for the collection, storage, maintenance, and dissemination of CHRI. The two primary methods the FBI uses to achieve this goal are the III correlation and the audit process.

III Correlation

States use the III correlation to identify their FBI-supported records in the III and take ownership of them. When a state requests a correlation, the FBI CJIS Division provides all records maintained by the FBI for the requesting state. Data are provided in segments so the state can easily compare FBI-maintained to state repository-maintained data. The state reviews the data to identify any records for which the state has as much information as or more information than the FBI. The state may take ownership of these records, allowing the FBI to reach out to the state for the state-maintained record as long as the state supports the purpose of the request. Because studies have shown states to have more up-to-date records (including additional information, such as dispositions), the FBI CJIS Division supports state outreach and the decentralization of CHRI.

Audit

The FBI audits each state central repository for compliance with III and NFF participation standards for CHRI use, dissemination, and security. The FBI CJIS Division auditors review and analyze methods used by the repository to administer policies and procedures mandated by various federal laws and policies. The auditors assess the performance of a repository in the areas of fingerprint identification, record content, III maintenance, record request responses, data quality, data use, data dissemination, and data security. The CJIS Division uses the same criteria to audit federal agencies, territories, tribes, and authorized users with access to FBI CJIS Division systems.

The CJIS Security Policy requires that each agency implement audit and accountability controls to ensure the lawful use and protection of CHRI. Security measures and adherence to FBI policies on the part of the agency and the CJIS Division ensure the information is protected. In addition, each federal agency and state central record repository must audit its own system and use of FBI systems. The FBI CJIS Division audits federal, state, territorial, and tribal agencies, as well as other authorized users, triennially.

The Privacy Act, 5 U.S.C. § 552a, allows CHRI to be provided to authorized agencies for non-criminal-justice purposes. These authorized agencies are required to maintain a system of records that establishes appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. The FBI CJIS Division auditors conduct both criminal justice and non-criminal-justice audits to

evaluate compliance with appropriate laws, policies, and regulations that pertain to the use, dissemination, maintenance, and security of CHRI. The audit helps to ensure the responsible use of the III and to address violations that may be detected.

CHR Improvement Efforts

As stated, all information submitted to the III is done voluntarily by federal, state, territorial, tribal, and local agencies. Missing dispositions and rap-sheet standardization are two areas in which the FBI continues to seek improvement.

Missing Dispositions

While collecting and sharing fingerprints and arrest details is a valuable tool for law enforcement agencies across the country, agencies often do not submit the final outcome of these arrests.

Dispositions are important to making CHRs effective. Missing dispositions lead to incomplete CHRs, which can cause problems for criminal justice agencies, non-criminal-justice agencies, and the subject of the record. Therefore, the FBI CJIS Division has developed a plan to obtain missing disposition information and complete as many records as possible.

Multiple efforts have been used to identify missing state and federal dispositions, including—

- collaborating with U.S. courts and U.S. attorney's offices
- hiring contractors to research and locate possible dispositions from public-facing court websites to update CHRs
- technical enhancements to make submitting dispositions to the FBI easier.

The disposition issue is a top priority for the FBI because dispositions are shared for employment and licensing adjudications, firearms background checks, Rap Back services, criminal investigations, and sentencing decisions. As mentioned, 28 C.F.R. § 20.37 provides that dispositions should be submitted within 120 days after they occur. The FBI CJIS Division has been working with federal, state, and tribal agencies to obtain missing dispositions and continues to provide updates and solutions to its partners through outreach efforts and the shared management process.

Rap-Sheet Standardization

The CHR, often referred to as a rap sheet, varies in format. For example, a CHR returned from the FBI is formatted differently from one returned from the NGI System state outreach or from an NFF-participating state. There have been discussions and studies on standardization, but no standard format is currently required for placement and content of biographic descriptors and CHRI.

The FBI CJIS Division has launched a project to identify reporting methods common to all federal and state agencies to streamline responses. The project goal is to improve the effectiveness of CHR reviews by standardizing the national CHR display. Rap-sheet standardization would streamline the review

process, helping the criminal justice and non-criminal-justice communities make better decisions relating to supervisory or custody data, sentencing, and adjudications for employment, licensing, or firearms purchases.

US 4. Accessing Criminal-History Record Data for Research Purposes

FBI Institutional Review Board

As a general matter, federal regulations prohibit federal agencies from engaging (or assisting with resources) in human subjects research without prior review and approval from a governing Institutional Review Board (IRB), whose job it is to protect the interests of the human subjects about whom the research relates. Depending upon the exact nature of any CHRI, metadata, or related information sought to be used, its public availability, the purposes for which it will be utilized and the method of its processing and availability, some activities involving such information may qualify as human subject "research" (a defined term) and may require prior IRB review and approval while other activities may qualify for an exemption from such review. For the DOJ and all of its components, including the FBI, those regulations are contained in 28 C.F.R. Part 46. Pursuant to this authority and internal policy, the FBI maintains an FBI IRB that is administered by the FBI Science and Technology Branch. In accordance with guidance from the U.S. Department of Health and Human Services, Office of Human Research Protections, researchers should seek a determination from a designated FBI IRB representative regarding the inclusion or exemption of their activities from the FBI IRB governance. Under the FBI policy, exemption and exclusion decisions are made by the FBI IRB Chair in consultation with the FBI IRB Counsel. When the FBI IRB reaches an exemption determination, it issues a written exemption ruling. On average, approvals and exemptions are issued by the FBI IRB within 33 days of its receipt of completed FBI IRB forms providing the necessary information to make a determination.

Researchers should keep in mind that the narrow role of the FBI IRB is to protect the interests, including privacy interests where applicable, of the human subjects about whom the research relates. As such, an FBI IRB approval or exemption determination resolves only that equity and does not qualify as authority to actually gain access to or use the FBI CHRI or other information. A separate review process exclusively controlled by the FBI Office of the General Counsel (OGC) under requirements controlled by different regulations is required to gain access to such information or data, assuming the proposed activity is either exempted or approved by the FBI IRB.

Access to the FBI CHRI for Research Purposes

The FBI OGC Criminal Justice Information Law Unit (CJILU) approves requests for access to CHRI for research purposes. Access to CHRI is governed by 28 U.S.C. § 534 and 28 C.F.R. Parts 20 and 22.

Title 28 U.S.C. § 534 charges the AG with the acquisition, collection, classification, and preservation of identification, criminal identification, crime, and other records. It also authorizes the exchange of records with, and for the official use of, "authorized officials of the Federal Government, including the United States Sentencing Commission, the States, including State sentencing commissions, Indian tribes, cities and penal and other institutions." The DOJ and federal courts have interpreted this language to restrict

access to CHRs to criminal justice agencies for criminal justice purposes and to federal agencies authorized to receive such records pursuant to a federal statute or executive order.

The FBI CHRI can be disseminated for research requests pursuant to 28 C.F.R. § 20.33(a), which authorizes sharing with criminal justice agencies[27] for criminal justice purposes;[28] research conducted under a specific federal statutory authorization; or research that is in accordance with 28 C.F.R. Part 22, which governs the use of research and statistical information obtained, collected, or produced either directly to the Bureau of Justice Assistance, the Office of Juvenile Justice and Delinquency Programs, the Bureau of Justice Statistics (BJS), the National Institute of Justice, or the Office of Justice Programs.

Prior to the transfer of CHRI, an Information Transfer Agreement (ITA) must be executed. For each agency, the ITA must be signed by an official representative who is authorized to execute such documents on behalf of and for the agency.

US 5. Using Criminal-History Data for Research

Government and non-government researchers, such as those from universities and private organizations, use criminal-history data from the FBI or an individual state repository to study the criminal careers and recidivism patterns of different types of offenders (e.g., adults released from prison or sex offenders who have completed a treatment program). For instance, researchers within a state's statistical analysis center use criminal-history data from their state to conduct research needed to inform state- and local-level policy and practice.[29] Research conducted by state agencies is typically limited to criminal-history data within their own state because these agencies do not have direct access to national criminal-history data from the FBI or criminal-history data from outside of their state.

In general, criminal-history records used for research are the same records used for operational purposes by police officers, judges, and corrections officials. However, certain records available for criminal justice purposes may not be available for research, such as those that are sealed or expunged and no longer publically available. In addition, crimes committed by juvenile offenders are generally not available in the criminal-history records obtained for research unless the offender was charged or tried as an adult.

Researchers must typically establish a data security agreement with the repository and use secure file transfer procedures to obtain the criminal-history data. When researchers are unable to access criminal-history data through the repository, some have been able to obtain criminal justice data directly from the local police departments or courts within a particular jurisdiction. While these data can provide comparable information found in the criminal-history data regarding a single stage in the criminal justice system (e.g., arrest or prosecution), they do not provide the comprehensive summary of a person's involvement with the criminal justice system.

[27] Criminal justice agency is defined in 28 C.F.R. § 20.3(g).
[28] Administration of criminal justice is defined in 28 C.F.R. 20.3(b).
[29] The Justice Research and Statistics Association (JRSA) website provides a directory of the Statistical Analysis Centers in the states and territories: http://www.jrsa.org/sac/index.html.

After obtaining the necessary approval to conduct a study, the researcher must supply the repository with identifying information on the study's sample of individuals (e.g., names, dates of birth, and state identification numbers) and request that the agency provide the criminal-history records on each person. Depending on the source of the criminal-history data, researchers can receive either individual paper records on each individual in the study or a single data file that contains the criminal-history data on the entire sample of offenders in the study. Because the content of the variables included in criminal-history records can vary widely across jurisdictions, a data extract received from a state repository or the FBI can require extensive work to transform the free-text fields (e.g., offense descriptions and summaries of case outcomes) into a research file with numeric codes and summary variables that can support the statistical analyses. Depending on the purpose of the study, researchers can use the arrest charge, court disposition, or incarceration information from the criminal-history records to examine criminal careers or measure recidivism. A new arrest following a criminal sanction is one of the most common measures of recidivism. Other common recidivism measures based on criminal-history records include a new court conviction or a return to prison.

Although certain restrictions may be imposed on the research to protect confidentiality, the personal identifiers used to obtain criminal-history data also provide the ability to link the records on the persons in the study to other criminal justice and non-criminal-justice data sources, such as mortality or employment, to conduct more in-depth multivariate analysis on the research results. For instance, when conducting studies using criminal-history data, researchers need to identify those offenders who were eligible to reoffend throughout the follow-up period. If a person dies before the end of the study, his or her lack of reoffending would be erroneously interpreted as not offending and artificially suppress the observed recidivism rate. To address this issue, researchers often use death information on the persons in the study subjects from the criminal-history records or other data sources to exclude those who died during the follow-up period from the recidivism analysis.

Research studies based on criminal-history records rely on fingerprint-verified records from the repositories. Criminal justice agencies are typically required by law to submit fingerprints to a central repository when a person is arrested for a felony or serious misdemeanor. However, the criteria for reporting arrests and dispositions to repositories varies by state. Some states also require the reporting of less serious offenses, violations, infractions, and traffic citations. Differences in criminal-history reporting practices across states can make it difficult to compare recidivism rates from state to state. For example, a state that is required to report certain less serious misdemeanors to the criminal-history repository may appear to have a higher recidivism rate than another state that is required to report only felonies and serious misdemeanors.

Certain federal agencies—including BJS, the Administrative Office of the U.S. Courts (AOUSA), the U.S. Sentencing Commission (USSC), and the BOP—are authorized to collect and analyze national (i.e., multi-state) criminal-history records obtained through the FBI's III System for the purpose of studying criminal offending and recidivism patterns. BJS's national recidivism studies of persons released from state prisons have been a primary source of information on the number and types of crimes persons commit prior to and following release from prison. The largest BJS recidivism study to date examined the offending patterns of state prisoners released in 30 states in 2005.[30] The AOUSA uses criminal-history

[30]More information on the BJS recidivism studies is available at https://www.bjs.gov/index.cfm?ty=dcdetail&iid=270.

data to study the effectiveness of federal community supervision programs and produces recidivism reports that help to inform the operations of the federal probation offices and other criminal justice agencies. To help inform sentencing practices, the USSC routinely uses criminal-history records to track the recidivism rates of various groups of offenders released from federal prison and those placed on federal probation. The BOP uses criminal-history records to assess the outcomes of federal prisoner reentry programs.

Research Report

Comparison of Criminal-History Information Systems in the United States and Other Countries

A Review of Systems in Australia, Canada, England and Wales, Germany, and the Netherlands

Jirka Taylor, Lucy Strang, Kristy Kruithof, Beau Kilmer, Fook Nederveen, Emma Disley, Lisa Wagner, and Jörg-Martin Jehle

RAND Social and Economic Well-Being

April 2020
Prepared for the Bureau of Justice Statistics

Contents

Preface

Criminal-history records are an important component of many criminal justice systems throughout the world and are used not only by law enforcement agencies but also by courts, corrections systems, and researchers. However, little is known about how the United States criminal-history information system compares with those in other industrialized countries. Practices relating to the collection, management, and quality control of criminal-history information vary across individual jurisdictions within the U.S. and between different countries.

The overarching objective of this project, sponsored by the Bureau of Justice Statistics, was to help fill the information gap described above and compare the criminal-history information system in the U.S. and other countries. The countries covered by this research were Australia, Canada, England and Wales, Germany, and the Netherlands. The research drew on consultations with subject matter experts in each country, complemented by document reviews and interviews with practitioners and researchers working in the area of criminal justice.

This work aimed to (1) provide insights into potential improvements of the accuracy, completeness, and timeliness of criminal-history records, along with their accessibility and utility to governmental and nongovernmental researchers and (2) offer lessons to government agencies in the U.S. and internationally. The primary audience for this report is practitioners managing or working with criminal-history record information, but it will be of interest to other stakeholder groups, including criminal justice researchers.

RAND Corporation's Social and Economic Well-Being division seeks to actively improve the health and social and economic well-being of populations and communities throughout the world. This research was conducted in the Justice Policy Program within RAND Social and Economic Well-Being. The program focuses on such topics as access to justice, policing, corrections, drug policy, and court system reform, as well as other policy concerns pertaining to public safety and criminal and civil justice. For more information, email justicepolicy@rand.org.

Tables

Figures

Boxes

Summary

A criminal-history record typically holds information about an individual's contacts with the criminal justice system, such as arrests, charges, court appearances, convictions, and sentences, as well as biographic data. It is an important component of many criminal justice systems around the world and is used not only by law enforcement agencies but also by courts, corrections, and researchers, including those outside the jurisdictions where the offense occurred.

However, little is known about how the United States criminal-history information system compares with those in other industrialized countries. Practices relating to the collection, management, and quality control of criminal-history information vary across individual jurisdictions within the U.S. and between different countries. A cross-national comparison of how countries develop and use criminal-history information may provide lessons that inform efforts to address and overcome challenges associated with the operation of criminal-history information systems. It may also highlight innovative practices that could be adopted in other countries with the aim of improving the functioning of individual national systems.

The overarching objective of this project, sponsored by the Bureau of Justice Statistics (BJS), was to help fill the information gap described above and compare the criminal-history information system in the U.S. and other countries. This work aimed to provide insights into potential improvements of the accuracy, completeness, and timeliness of criminal-history records, along with their accessibility and utility to governmental and nongovernmental researchers and to offer lessons to government agencies in the U.S. and internationally.

The study aimed to document and compare the answers to the following research questions:

1. What are the characteristics of the national criminal-history information system? What data does it hold and who provides the data?
2. What is done to ensure data quality and completeness of data held by the national criminal-history information system?
3. Who has access to the criminal-history information for operational and civil purposes?
4. How are criminal-history record data used for research purposes?

In addition to the U.S., the countries selected for the study were

- Australia
- Canada
- England and Wales[1]
- Germany
- the Netherlands.

[1] As a result of a long process of devolution, the United Kingdom's government is responsible for criminal justice matters only in England and Wales. Scotland and Northern Ireland each has its own, separate criminal justice system, although there are commonalities and links between the systems.

The countries were selected on the basis of objective criteria (e.g., relatively large countries with advanced information systems), coupled with a consideration of the feasibility of successful collection of data pertaining to each jurisdiction. In each country, RAND, where necessary with support from BJS, established collaborations with subject matter experts. These experts were either government representatives whose portfolio involved working with the national criminal-history information system or academic researchers with extensive experience working with national criminal-history data. In addition to experts' input, information was gathered from two other sources. First, a review of existing literature and official documentation was conducted pertaining to national criminal-history information systems. The second data collection activity was a series of interviews with key subject matter experts from the countries. The interviewees were either government officials in a position to comment on the country's criminal-history information system or academic researchers who have worked with national criminal-history data.

In parallel with the development of the country chapters presented in this report, the FBI prepared a chapter on the U.S. national criminal-history information system that includes contributions from BJS, broadly mirroring the standardized chapters prepared by RAND on the other countries. Information from this U.S. chapter was used by RAND to inform the summary chapter comparing the U.S. system to those in the other countries.

Characteristics of National Criminal Record Information Systems

There are discernible differences across all the studied countries in the functions that their national criminal record information systems (CRIS) are designed to perform. Two broad organizational approaches can be distinguished. In Australia, Canada, England and Wales, and the U.S., the national systems are maintained by specialized departments of law enforcement or criminal intelligence agencies and are designed to capture information on the entire history of an individual's interaction with the criminal justice system. In these countries, data typically start being collected at the moment of arrest or when a person is charged by the police with an offense. The national CRIS in these countries also contains or is linked to databases containing noncriminal-history information, such as a database of missing persons.

By contrast, in the Netherlands and Germany, the national systems are maintained by specialized governmental agencies falling under the responsibility of the national Ministry of Justice. In these countries, data collection for the national CRIS starts later, as individuals progress in the criminal justice system, and is not initiated by police agencies. In the Netherlands, individuals need to be prosecuted for the alleged offense, and in Germany, individuals need to be convicted for their records to appear in the national system. One exception to this rule in Germany are prosecutions and court disposals of juvenile cases (with or without the imposition of a conditional measure), which are also recorded.

Content of National Criminal Record Information Systems

The variation in the content of national CRIS in the countries mirrors the differences in what type of agency is responsible for maintaining the national system, as discussed above. In Australia, Canada, England and Wales, and the U.S., police agencies are the creators of criminal records, as well as one of the primary (although not necessarily the only) sources of data for the national CRIS. In Australia, Canada, and in some instances England and Wales, police agencies are responsible even for the provision of data originated by other criminal justice agencies, such as court dispositions. By contrast, in the Netherlands and Germany, the two countries' national systems primarily rely on data from public prosecutors and courts, respectively, although as in the other countries, additional agencies also provide information to the system.

Criminal-history records in all the countries contain the following information: (1) personal information, such as name(s) and date and place of birth; (2) information on the offense, such as date and applicable legal provisions; and (3) information on the sentence imposed, including any suspensions, conditions, and subsequent modifications. However, within these categories, some variation and unique features can be observed, which again follow the differences between systems informed primarily by law enforcement and criminal intelligence agencies and those maintained by other governmental agencies.

In all the countries, data are generally provided to the national CRIS by originating agencies via a standardized electronic reporting system, although some manual input may take place in limited circumstances. In all jurisdictions, the information submitted to the national system typically does not represent the totality of data pertaining to the criminal record that are held by originating agencies, although the extent of this phenomenon varies across countries.

Data retention policies are another area where there is variation across the countries. Germany and the Netherlands differ from the other countries and may retain data for a comparatively shorter period. In Germany, the length of the retention period depends on the sentence imposed, with the rule that longer sentences are generally associated with longer retention periods. In the Netherlands, the length of the retention period depends on the offense, with a similar rule that records for more serious offenses are retained longer. By contrast, in the other countries, criminal records will generally be retained for a much longer period—the countries either set an age limit that substantially exceeds the country's life expectancy or routinely do not delete criminal records at all.

Access to the System

Across all the countries, access to criminal-history information systems is granted to law enforcement and other criminal justice agencies to support their operations. Under certain conditions, access may also be provided to other selected government agencies, although the extent of this provision varies across the countries. Provisions also exist for the international sharing of data. Among the countries studied, one of the most advanced and formalized

frameworks for cross-country sharing of criminal-history data is established in the European countries, which can use the European Criminal Records Information System (ECRIS). This system obliges European Union (EU) member states to notify other member states regarding the criminal history of their citizens and to respond to queries received from other member states. These exchanges of information make use of reference tables for offenses and sentences, which serve to approximate the criminal laws of individual member states.

The type of user agency typically guides two aspects of access rights to national criminal-history databases. First, it frequently determines what type of information user agencies can access, with certain content available only to specific agencies. Second, the identity of a given user agency may determine whether it can edit existing criminal records held in the national system or is restricted to read-only privileges, which tends to be common particularly for noncriminal justice agencies.

In addition, all the studied countries allow individuals to check their own records for information held about them, and the countries provide background checks for such purposes as employment, visa applications, and adoption applications. Individuals in all the countries can file an application for a record check, either with the system operators directly or via accredited checking agencies. For all the countries, the level of disclosure may depend on the offense history and the type of check being performed. Countries performing criminal-history checks also offer enhanced versions for individuals intending to work with children or vulnerable people. These enhanced checks can involve more thorough searches of existing data or be subject to stricter disclosure rules.

Access to criminal-history data is granted to researchers in all the countries included in this study, although the level of access varies widely. Typically, access may be approved for specific research activities that may provide a benefit to society and inform practice or policymaking.

Data Quality and Completeness

Across all the countries, there are common challenges with achieving data quality and some that are specific to the jurisdiction. In Australia, Canada, England and Wales, and the U.S., ensuring the quality of data held in the systems is the responsibility of the agency that originally entered the information. In Germany and the Netherlands, this responsibility rests with the agency that maintains the centralized system, but in both countries, the central authorities work with the originating agencies to resolve data issues.

Overall, four types of data quality and completeness challenges were identified across the countries. The first issue relates to the complexities of gathering data from multiple state and local jurisdictions, such as variable data formats, and variation in the type of information that state and territorial agencies share. A second challenge is the transfer of data from originating agencies to the national system, giving rise to such issues as missing dispositions or inaccuracies during the receipt and registration of data. A third issue is aging technological infrastructure.

And fourth, the limited scope of information held in national systems can represent a challenge. However, issues pertaining to the scope of information recorded are products of the legal framework governing the respective national systems and do not represent deficiencies on the part of the system's functioning or that of its users.

Various approaches to ensuring data quality in these systems were identified in the study's countries, often driven by the nature of the data quality issues experienced in each jurisdiction. The first group of efforts revolves around checking the accuracy and quality of submitted data. The second group of efforts addresses issues with data transfer and gaps in the provision of information from originating agencies. In addition, all the countries have put into place processes to audit the quality of the data held in the centralized systems.

Acknowledgments

We are deeply indebted to our country-level experts: Anna Ferrante (Curtin University, Australia), Don Weatherburn (New South Wales Bureau of Crime Statistics and Research, Australia), Martin Bouchard (Simon Fraser University, Canada), Bert Götting (Federal Office of Justice, Germany), Gijs Weijters (Research and Documentation Centre, Ministry of Justice and Security, the Netherlands), and Jack Cattell (Get the Data, United Kingdom).

We would also like to thank the key informants who shared their experiences and insights with us during interviews. We are also very grateful for the detailed feedback we received from our quality assurance reviewers, Stefan Harrendorf (University of Greifswald, Germany) and Stijn Hoorens (RAND Europe, Belgium). Mariel Alper and Matthew Durose from the Bureau of Justice Statistics provided great advice and helped steer us through the study, and their colleagues Devon Adams and Howard Snyder offered valuable insights and feedback on various drafts and presentations. A team from the Federal Bureau of Investigation, Criminal Justice Information Services Division, developed a chapter on the U.S. information system, which directly informed this report and provided very helpful comments on earlier drafts and presentations. Lastly, we would like to thank the Canadian Criminal Real Time Identification Services of the Royal Canadian Mounted Police for their useful feedback on the Canadian chapter.

Abbreviations

ABS	Australian Bureau of Statistics (AUS)
ACIC	Australian Crime and Intelligence Commission (AUS)
ACT	Australian Capital Territory (AUS)
AFP	Australian Federal Police (AUS)
AIC	Australian Institute of Criminology (AUS)
AUS	Australia
BfJ	Bundesamt für Justiz (Federal Office of Justice) (DEU)
BJS	Bureau of Justice Statistics (USA)
BKA	Bundeskriminalamt (Federal Criminal Police Agency) (DEU)
BKAG	Bundeskriminalamtgesetz (Federal Criminal Police Act) (DEU)
BOCSAR	Bureau of Crime Statistics and Research (AUS)
BRP	Basisregistratie Personen (Personal Records Database) (NLD)
BSN	burgerservicenummer (citizen service number) (NLD)
BTP	British Transport Police (E&W)
BVH	Basisvoorziening Handhaving (Primary Information Provision for Law Enforcement) (NLD)
BVI	Basisvoorziening Informatie (Primary Information Provision Database) (NLD)
BZR	Bundeszentralregister (Federal Central Criminal Register) (DEU)
BZRG	Bundeszentralregistergesetz (Federal Central Criminal Register Act) (DEU)
CAN	Canada
CCRTIS	Canadian Criminal Real Time Identification Services (CAN)
CDPP	Commonwealth Director of Public Prosecutions (AUS)
CFRO	Canadian Firearms Registry On-line (CAN)
CJIM	Criminal Justice Information Modernization (CAN)
CNI	Central Names Index (AUS)
CNI	Criminal Name Index (CAN)
CPIC	Canadian Police Information Centre (CAN)
CPS	Crown Prosecution Service (E&W)
CR	criminal record
CRIS	criminal record information systems
CRO	Criminal Records Office (E&W)
CRS	Criminal Record Synopsis (CAN)
CSC	Correctional Service of Canada (CAN)
DBS	Disclosure and Barring Service (E&W)
DEU	Germany

DJI	Dienst Justitiële Inrichtingen (Custodial Institutions Agency) (NLD)
DVLA	Driver Vehicle Licensing Agency (E&W)
E&W	England and Wales
ECRIS	European Criminal Records Information System
EEA	European Economic Area
FPS	fingerprint serial number (CAN)
HMIC	Her Majesty's Inspectorate of Constabulary (E&W)
HMICFRS	Her Majesty's Inspectorate of the Constabulary and Fire & Rescue Services (E&W)
HMPPS	Her Majesty's Prison and Probation Service (E&W)
ICPC	International Child Protection Certificate (E&W)
ICT	information and communication technology
III	Interstate Identification Index (USA)
INPOL	central police information system (DEU)
JDS	Judicial Documentation System (NLD)
JGG	Jugendgerichtsgesetz (Act on Juvenile Courts) (DEU)
JustID	Judicial Information Service (NLD)
MIAP	Ministry of Justice Information Access Panel (E&W)
MOJ	Ministry of Justice (E&W)
NAFIS	National Automated Fingerprint Identification System (AUS)
NCA	National Crime Agency (E&W)
NCIDD	National Criminal Investigation DNA Database (AUS)
NCOS	National Child Offender System (AUS)
NDNAD	National DNA Database (E&W)
NGI	Next Generation Identification (USA)
NIS	National Identification Service (E&W)
NLD	The Netherlands
NPCC	National Police Chiefs' Council (E&W)
NPCS	National Police Checking Service (AUS)
NPRS	National Police Reference Service (AUS)
NRCR	National Repository of Criminal Records (CAN)
NSW	New South Wales
OAIC	Office of the Australian Information Commissioner (AUS)
OBJD	Onderzoek- en Beleidsdatabase Justitiële Documentatie (Research and Policy Database for Judicial Documentation) (NLD)
ODPP	Office of the Director of Public Prosecutions (AUS)
OI	Offender Index (E&W)
OM	Openbaar Ministerie (Public Prosecution Service) (NLD)
ONS	Office for National Statistics (E&W)
OPP	Ontario Provincial Police (CAN)

PBC Parole Board of Canada (CAN)
PDS Persoonsdossier Systeem (Personal Document System) (NLD)
PIAP PNC Information Access Panel (E&W)
PNC Police National Computer (E&W)
PNCID Police National Computer Identity Number (E&W)
POM royal prerogative of mercy (AUS)
PPSC Public Prosecution Service of Canada (CAN)
PStG Personenstandsgesetz (Civil Status Act) (DEU)
QAR quality assurance review (CAN)
RCMP Royal Canadian Mounted Police (CAN)
RNC Royal Newfoundland Constabulary (CAN)
SKDB Strafrechtsketendatabank (Criminal Justice Chain Database) (NLD)
SIBs Social Impact Bonds (E&W)
SQ Sûreté du Québec (CAN)
StGB Strafgesetzbuch (Criminal Code) (DEU)
StPO Strafprozessordnung (Rules of Criminal Procedure) (DEU)
USA United States of America
VOG Verklaring Omtrent Gedrag (certificate of conduct) (NLD)
WODC Wetenschappelijk Onderzoek- en Documentatiecentrum (Research and Documentation Centre) (NLD)
ZStV Zentrales Staatsanwaltliches Verfahrensregister (Central Register of Criminal Proceedings) (DEU)

1. Introduction

A criminal-history record typically holds information about an individual's contacts with the criminal justice system, such as arrests, charges, court appearances, convictions, and sentences, as well as biographic data. It is an important component of many criminal justice systems around the world and is used not only by law enforcement agencies but also by courts, corrections systems, and researchers, including those outside the jurisdictions where the offense occurred (Jacobs, 2015).

The use of criminal-history information can take numerous forms. A prior arrest may drive a decision to detain rather than release an individual upon a new infraction (Fitzgerald O'Reilly, 2018; Kim et al., 2018), and prior convictions may inform sentencing for new crimes (Monahan and Skeem, 2016). Criminal-history records may also be used to determine eligibility in such areas as employment, gun ownership, or business licensing (Neighly and Emsellem, 2013). Limitations on criminal-history data collection, retention, and sharing, as well as options to expunge records, can be put in place to facilitate individuals' reentry and rehabilitation (Adams, Chen, and Chapman, 2017; Love, 2002; Maruna, 2011). Criminal-history information is utilized in research covering such areas as reoffending, the functioning of the criminal justice system, or the effectiveness of various criminal justice interventions (Drake and Fumia, 2017; Marshall, 2018; Myrent, 2019; Spohn, 2015; Vuolo, Lageson, and Uggen, 2017). To collect criminal-history information, individual jurisdictions maintain dedicated information systems, although their design and operationalization, as well as mode of use, differ across jurisdictions (Corda, 2018; Jacobs, 2015; Jacobs and Larrauri, 2015).

Further, the collection and maintenance of criminal-history information also raise questions regarding privacy and data protection (Jacobs 2006, 2015; Kurtovic and Rovira, 2017). National authorities need to balance on the one hand the needs of the criminal justice system and the objective of keeping communities safe and on the other individuals' right to privacy (Larrauri, 2014). This is reflected in cross-national differences in the extent of data collected, their retention, and access arrangements (Lapp, 2016). For instance, Herzog-Evans (2011) offers a broad categorization of countries into "right to know" (i.e., those with broad access to criminal records) and "right to be forgotten" (i.e., those with more restrictive rules).

In the U.S., all 50 states and the District of Columbia collect arrest information from local law enforcement agencies, which is later matched with adjudication and sentencing information. Each state maintains an independent criminal-history records database, and states are responsible for determining what information is stored in their systems. As a result, these state repositories have their own structure and characteristics. All states and the District of Columbia also provide records of persons arrested for felonies and serious misdemeanors to the Federal Bureau of Investigation (FBI) for inclusion in the Interstate Identification Index (III). III functions as a

pointer system to the state systems, maintaining an index of any state and federal identification numbers assigned to an individual. III is used by criminal justice agencies across the U.S. to access national arrest records, providing information that is pulled from the state systems. As of December 2016, the 50 U.S. states, Puerto Rico, and Guam reported holding criminal-history files on more than 110 million persons (Goggins and DeBacco, 2018).

In summary, criminal-history information systems are an essential resource for a range of operational, civilian, and research purposes, and the contents of criminal-history information systems have important implications for individual rights and freedoms. However, little is known about how the U.S. criminal-history information system compares with those in other industrialized countries. Practices relating to the collection, management, and quality control of criminal-history information vary across individual jurisdictions within the U.S. and between different countries. A cross-national comparison of how countries develop and use criminal-history information may provide lessons that inform efforts to address and overcome challenges associated with the operation of criminal-history information systems. It may also highlight innovative practices that could be adopted in other countries with the aim of improving the functioning of individual national systems.

Study Objectives

The main objective of this study, sponsored by the Bureau of Justice Statistics (BJS), was to help fill the information gap described above and compare the criminal-history information systems in the U.S. and other countries. This work aimed to provide insights into potential improvements of the accuracy, completeness, and timeliness of criminal-history records, along with their accessibility and utility to governmental and nongovernmental researchers and to offer lessons to government agencies in the U.S. and internationally.

The study aimed to document and compare the answers to the following research questions:

1. What are the characteristics of the national criminal-history information system? What data does it hold and who provides the data?
2. What is done to ensure data quality and completeness of data held by the national criminal-history information system?
3. Who has access to the criminal-history information for operational and civil purposes?
4. How are criminal-history record data used for research purposes?

Importantly, the goal of the international comparison was to shed light on variations in the way criminal-history information systems are designed and operated. As part of this comparison, this report comments on the trade-offs and considerations associated with individual characteristics and features of national information systems. However, the study did not aim to offer recommendations or lessons for any national authority; nor did it set out to comment on whether any features are more desirable than others.

In addition to the U.S., the countries selected for the study were

- Australia
- Canada
- England and Wales[2]
- Germany
- the Netherlands.

The selection of these countries was based on a combination of criteria designed to ensure that the study may offer innovative and transferrable lessons for the U.S. and other contexts. First, the countries serve relatively large populations—the smallest country in the sample, the Netherlands, has over 17 million inhabitants. Second, the countries' national information systems incorporate a high degree of automation, either in data collection or data retrieval. Third, all countries collect biometric information on individuals involved with the criminal justice system, even if, in some instances, this information is not directly available in the national criminal-history information system and must be accessed via a separate database. Fourth, all countries accumulate criminal-history information from multiple components within the criminal justice system. Fifth, the selection includes multiple countries with a federal system of government. As multiple countries potentially meet these criteria, the final selection of countries also took into account technical considerations surrounding data availability, language skills of the RAND team, and access to local subject matter experts via RAND's professional networks for consultation during the project.

Methodology

In each country, RAND, with support from BJS where necessary, established collaborations with subject matter experts. These experts were either government representatives whose portfolio involved working with the national criminal-history information system or academic researchers with extensive experience in working with national criminal-history data.

In consultation with BJS, RAND developed a standardized outline for each country chapter (see Appendix A). The outline served as the basis for the data collection efforts described below.

The first step in developing country chapter content was a consultation with country experts to clarify the scope of the chapter, discuss any issues likely to be covered, and identify sources to review and potential interviewees.

In addition to experts' input, information was gathered from two other sources. First, a review of existing literature and official documentation was conducted pertaining to the various national criminal-history information systems. These sources included academic articles,

[2] As a result of a long process of devolution, the United Kingdom's government is responsible for criminal justice matters only in England and Wales. Scotland and Northern Ireland each has its own, separate criminal justice system, although there are commonalities and links between the systems.

applicable laws and regulations, government publications, and others (e.g., reports from nongovernmental organizations).

The second data collection activity was a series of interviews with key subject matter experts from the included countries. The interviewees were either government officials in a position to comment on the country's criminal-history information system or academic researchers who have worked with national criminal-history data. While the interviews conducted by RAND followed a structure similar to the standardized chapter outline, there was no unified topic guide for the interviews. Each discussion was tailored to the specific country context and to address questions raised in the data collection process. In some instances, country experts offered to consult with colleagues or their national authorities to answer questions raised during the project. Elsewhere, RAND researchers (directly or with the facilitation of country experts) submitted written questions to national authorities responsible for the country's criminal-history information system.

In parallel with the development of the country chapters presented in this report, the FBI prepared a chapter on the U.S. national criminal-history information system. It includes contributions from BJS, broadly mirroring the standardized chapter prepared by RAND on the other countries. RAND used information from the U.S. chapter to construct a series of comparative tables, intended to summarize the characteristics of information systems in the U.S. and the other countries and to highlight notable similarities and points of divergence. These tables formed the basis of the comparative chapter presented in this report (see Chapter 7). Further details on the study's methodology are provided in Appendix B.

Limitations

This report is subject to two notable limitations. First, the scope of this report was limited to national criminal-history information systems (i.e., systems maintained by the central government and containing as complete a record of individuals' criminal histories as possible). This report does not examine other databases that may hold some information on individuals involved with the criminal justice system (e.g., prosecutor databases), although this report discusses additional databases and their relationship to the main national information system as appropriate. This focus also excludes information systems maintained by lower levels of government (e.g., databases operated by provincial and territorial authorities in Canada). Again, this report makes references to databases existing at other levels of government where appropriate.

Second, there are typically few publicly available official assessments of the quality and completeness of data held by national information systems that could be used in this report. Relatedly, while efforts to address existing data challenges have been documented, there is comparatively little information available on the effectiveness of these efforts. To address this challenge, this report draws extensively on input from subject matter experts as the best available

source of information to provide an assessment of data quality and completeness in each country chapter. These testimonies represent a novel source of information that has not been documented elsewhere.

Structure of This Report

The remainder of this report is structured as follows. Chapters 2 through 6 present information on the systems in Australia, Canada, England and Wales, Germany, and the Netherlands. Each of these chapters is structured in line with the unified chapter template (see Appendix A). Chapter 7 highlights and summarizes the key similarities and differences between the U.S. and the other selected countries and offers some concluding remarks.

2. Australia

Key Findings

- Australia is a federation of six states and two self-governing territories that have their own constitutions, parliaments, and laws. As such, there are nine criminal justice systems in Australia: one federal (or Commonwealth) system and eight state or territory systems.
- Each jurisdiction has separate and independent systems of courts, police, and corrective and treatment services. Across the jurisdictions, there are some common legal principles, but they each differ in definitions of offenses, their relative seriousness, available defenses, and prescribed punishments.
- Each state, territory, and federal police force maintains its own criminal-history information system, which in some jurisdictions may be linked with their local courts. Each police force retains ownership of the data that are created within their system although some of the data can be accessed through a national police information system, called the National Police Reference Service (NPRS).
- The Australian Crime and Intelligence Commission (ACIC), a national law enforcement agency with investigative and information-sharing services, is responsible for maintaining the NPRS and facilitates police access to it.
- The NPRS maintains records on persons of interest and includes criminal records from all Australian police jurisdictions. The NPRS provides law enforcement officers across the country with a minimum amount of criminal-history data that can be of use operationally.
- ACIC does not create any of the records held in the NPRS system. These originate from the various police jurisdictions in Australia, which input their data directly into the national system through an automated process.
- The NPRS is used by police agencies across Australia for operational purposes, such as informing police investigations or dealing with persons of interest. In addition, there is a small number of non-law-enforcement agencies that can access the NPRS directly.
- The NPRS is also used to support the National Police Checking Service (NPCS), which provides individuals with a police check that may be required when applying for a job, working with children, citizenship, or appointment to a position of trust, known as a Nationally Coordinated Criminal History Check.
- Historically, criminal-history information held in the national system has not been used for research purposes. However, in late 2017, the Australian Institute of Criminology (AIC), the national crime and justice research center, was granted access to NPRS data for a research project on organized crime offenders. The AIC's research activity using NPRS data may soon expand to other areas, such as domestic violence offenses.
- Rules around the retention of criminal-history information are a matter for the police jurisdiction where a record was created. Generally, information relating to interactions between police and a person of interest, any charges, and any subsequent conviction collected on policing systems is not routinely deleted by forces.
- All police forces are responsible for the quality of their own data; ACIC does not audit or change the data held on the national system.
- A small number of issues with the data have been identified. Multiple nominal records pertaining to the same individual are known to exist in the NPRS. This may arise from police forces not receiving complete or accurate information relating to a court outcome or when police were not provided with information relating to further sentencing, appeals, or any other decisions made subsequent to the initial outcome.
- With respect to the NPCS checks, the application of state and territory disclosure rules can occasionally lead to inconsistencies in the release of criminal-history information across jurisdictions.

AUS 1. Overview of the Country and Criminal Justice System

AUS 1.1 Political and Constitutional System

Australia is a constitutional monarchy and a participatory democracy, with a population of slightly over 25 million people as of 2018 (ABS, 2019). The country is a federation of six states and two self-governing territories that have their own constitutions, parliaments, and laws. As such, there is no single criminal justice system in Australia but rather nine: one federal system and eight state and territory systems. Under the Australian Constitution, the Commonwealth government (the federal government) may make laws on such matters as trade and commerce, taxation, defense, and external affairs. The states and territories have responsibility for all other matters. Therefore, most of the administration of justice takes place in these subnational jurisdictions, each of which has a separate and independent system of courts, police, and corrective and treatment services. Across the jurisdictions, there are some common legal principles, but they each differ in definitions of offenses, their relative seriousness, available defenses, and prescribed punishments. As a result, inconsistencies arise in the charging, convicting, and sentencing of individuals across the states and territories, which can also pose challenges in the use of criminal-history data across jurisdictions (explored further in Section AUS 3 below) (Daly and Sarre, 2017).

AUS 1.2 Criminal Code and Procedure

Australian criminal law was originally based in English common law, which is derived from precedential decisions of relevant courts. The states of New South Wales (NSW), South Australia, and Victoria remain common law jurisdictions. This means that, although these states have passed legislation listing the most common offenses and the available penalties, the legislation does not exhaustively define all the elements of the relevant offense. In the Australian Capital Territory (ACT), the Northern Territory, Queensland, Tasmania, and Western Australia, as well as at the federal level, criminal law has been wholly codified in legislation. Across the various jurisdictions, there are generally two types of offenses. *Summary offenses* are usually considered to be less serious crimes, such as motoring offenses, minor assaults, property damage, or offensive behavior. This type of matter can be heard in the magistrates or local court rather than by a judge and jury in a higher court and can be heard in the absence of the defendant. *Indictable offenses* are more serious offenses, such as aggravated burglary, indecent assault, or murder. These matters are usually heard initially in the magistrates or local court for a committal hearing and then sent to a higher court, such as a district, county, or supreme court for a trial before a judge. They cannot be heard in the absence of the defendant.

AUS 1.3 Court Dispositions and Penal Sanctions

There is an array of punishments available to the courts, which vary somewhat according to jurisdiction. In NSW, for example, an offender may be sentenced to a period of imprisonment in a correctional center (for adult offenders) or a juvenile detention center. Other options include intensive correction orders, which are served under strict supervision in the community, home detention under supervision, or electronic monitoring. Noncustodial sentences include community service orders, requiring the offender to perform unpaid work in the community; good behavior bonds, which direct an offender to be of "good behavior" for a certain period; disqualification from driving (for driving offenses); fines or monetary orders for court costs, witness expenses, or compensation for the victim; and apprehended violence orders, which prohibit certain behavior toward a protected person.

In addition, there are a number of diversionary programs for certain defendants who may be experiencing such issues as alcohol or drug dependency, mental illness, homelessness, or extreme poverty. In these matters, the judicial officer will adjourn the case for the duration of the defendant's participation in the program. For example, NSW's drug court offers special programs for drug dependent adults who are charged with criminal offenses by diverting them into programs designed to address their dependency issues. At the local court, the Extra Offender Management Service focuses on addressing the characteristics or issues of the offender that directly relate to his or her likelihood of reoffending. The Traffic Offender Intervention Program is available to offenders following a guilty plea or verdict and provides a community-based road-safety education program.

AUS 1.4 Agencies in the Criminal Justice Chain and Their Roles

Law enforcement: At the federal level, the primary law enforcement agency is the Australian Federal Police (AFP), which in practice limits its focus to such offenses as terrorism or transnational, serious, and organized crime. AFP is also responsible for local law enforcement in the Australian Capital Territory, where the federal government agencies are predominantly based. In addition to AFP, there a number of other national agencies that have enforcement powers in specific areas, such as national security (e.g., the Australian Security Intelligence Organisation) and white-collar crime (e.g., the Australian Competition and Consumer Commission and the Australian Securities and Investments Commission). Except for the Australian Capital Territory, all states and the Northern Territory have a single and separate statewide or territorywide police force, and these police forces perform the bulk of policing in Australia. They are responsible for enforcing state and territory laws and also assume responsibility for the enforcement of various federal laws, alongside AFP and other federal officers. The police generally determine the charges against a defendant and typically have responsibility for prosecuting less serious charges in some courts, such as magistrates courts and children's courts.

Prosecution: The responsibility to prosecute federal offenses lies with the Commonwealth Director of Public Prosecutions (CDPP), who may prosecute such matters in the magistrates courts (depending on the matter), the district or county courts, supreme and mental health courts, the courts of appeal, and the High Court of Australia. However, some federal offenses may also be prosecuted at the state or territory level by local prosecutors, in certain circumstances. For example, it is common practice for state and territory courts to hear a charge by state prosecutors of "using a carriage service to menace or harass," which is a federal offense, as part of a domestic violence case involving other state laws. Serious state- or territory-level offenses are prosecuted by the jurisdiction's own Office of the Director of Public Prosecutions (ODPP). As noted above, for less serious offenses, prosecution is most often carried out by police officers who have received training for the task. Prosecutors may be granted wide discretion in determining whether to prosecute charges and may negotiate with a defendant's legal representative on the seriousness of the charges in return for a guilty plea.

Courts: Across Australian courts, judges and magistrates are appointed by the government of the relevant jurisdiction, without the participation of the judiciary or the public. Although there is variation between the states and territories in terms of the hierarchy of their courts and the limits of their jurisdiction, the High Court of Australia has appellate jurisdiction over all other courts, as well as some original jurisdiction in certain matters. High Court decisions are binding on all Australian courts. Furthermore, all states and territories have a supreme court, the highest court within their jurisdictions. All states except Tasmania have two further levels of courts: the district or county court, which deals with most criminal trials for less serious indictable offenses, and the magistrates or local court, which typically handles summary matters. Tasmania and the two self-governing territories have only one level of court below their supreme courts.

The federal court does not have criminal jurisdiction. Instead, federal criminal charges are heard in state courts, which are given jurisdiction to hear federal criminal proceedings, and are prosecuted by CDPP. As noted above, state and territory courts can also sometimes rule on matters subject to federal legislation. In addition, all states and territories have specialized children's courts (called youth, juvenile, or children's courts, depending on the jurisdiction), which deal with offenses committed by young people, usually between the ages of 10 and 16 or 17 years.

AUS 1.5 Size of Criminal Justice System

According to the most recent statistics presented in the Recorded Crime—Offenders collection, the national number of offenders (persons aged ten years and over who have a case brought against them by the police) in 2016–2017 was 413,894, corresponding to a rate of 19 offenses per 1,000 population (ABS, 2019). Across the country, approximately 70 percent of those accused of criminal offenses pleaded guilty to the charge, according to data from 2013–2014 (Durnian, 2015). Generally, the courts consider an early guilty plea a mitigating factor in sentencing, reducing its severity (Sentencing Advisory Council, 2018). The most recent figures

from the Australian Bureau of Statistics from January to March 2019 show that the average daily number of full-time prisoners in Australia was 43,320, corresponding to a rate of 221 per 100,000 adult population. Approximately one-third of individuals in full-time custody were unsentenced (ABS, 2019).

AUS 2. Summary of Criminal-History Record System

AUS 2.1 History and Organizational Management

Criminal-history information sharing is facilitated by ACIC, a national law enforcement agency with a number of investigative and information-sharing responsibilities to its national and international partners.[3] ACIC was formed in 2016, the result of a merger between two federal agencies, the Australian Crime Commission and CrimTrac, and sits within the Department of Home Affairs. ACIC maintains the NPRS, a database of persons of interest, including criminal records from all Australian police jurisdictions. The NPRS provides law enforcement officers across the country with a minimum amount of criminal-history data that can be of use operationally (see AUS 2.2 below). In particular, the system was intended to assist with officer safety by providing information on how an individual may behave with the police and to assist with operational decisionmaking, for example, by advising that an individual has an outstanding warrant and should be taken into custody.

The NPRS is also used to support the NPCS, which provides individuals with a police check that may be required when applying for a job, working with children, citizenship, or appointment to a position of trust, known as a Nationally Coordinated Criminal History Check (see Section AUS 2.4 below).

ACIC does not create any of the records held in its system. Rather, these originate from the various police jurisdictions in Australia, which input their data directly into the national system through an automated process. Records held in the NPRS are not copies of the records held in local systems but a version of the records with only some of the data transferred (explained below). As of 2018, ACIC's system contained around 11 million nominal records (i.e., records relating to a specific individual). However, the number of people with criminal records in Australia is substantially fewer. There are two main reasons behind this discrepancy. First, as noted above, the NPRS is a *persons-of-interest* database and as such also contains records that do not relate to criminal history. This includes information on missing persons and unidentified persons and bodies. Second, there is an absence of *identity resolution* in the records. If an individual in a particular state has had multiple interactions with the police, it is likely but not

[3] There is little publicly available information on the Australian system, conceivably at least partly due to its recency. For that reason, this section, along with Sections AUS 3 and 4, primarily draws on interviews with Australian policy representatives and practitioners who are either familiar with or involved in the management of the system.

certain that these records will be linked by biometric data and collated into a single record. If no such links have been made, there may be multiple nominal records for a single individual. Furthermore, if an individual has criminal records in multiple states, these records may not be linked in the national system. This may occur, for example, if the individual was not fingerprinted by police or if there was an error with the individual's Central Name Index (CNI) number. This is discussed further in Section AUS 3.

Creating a Record

The process to create records and transmit them to the national database varies across jurisdictions. Typically, when an individual is arrested and charged, the relevant police force creates the charge in their own records management system. However, some police forces may create a record for an individual once a criminal investigation begins and before the person is arrested. Fingerprints are usually but not always taken at the point of arrest and charge. In some cases, a suspect may be fingerprinted before any arrest has taken place. Every individual with a record is assigned a unique CNI number, and if their fingerprints have been taken, these will be run against the National Automated Fingerprint Identification System (NAFIS). If an existing record on an individual is found, the new record can be manually linked to the existing record using the CNI number; this process is not automated.

Each police force has its own tailored information system. These systems typically are linked automatically with the relevant court system in their jurisdiction to record the charge in the court database. Once the criminal matter is heard in court, records are usually returned electronically to the police system by the courts, prosecutors, and other governmental agencies that conduct prosecutions. Subsequent decisions, such as further sentencing or appeals, should also be updated by the courts and transmitted to the local police force. However, there are a small number of courts that still rely on paper records that have to be processed manually by the police.

Once the police system receives information from a court on the outcome of a case, the relevant record is updated in the local police system. The time required to update a record with the court information varies across the state systems. In some states and territories, this process may be completed within a day; where courts are still reliant on paper files, a time lag may be generated while the files are transported to the police. Some criminal matters can be initiated by nonpolice agencies, such as environmental, health, and animal protection organizations, from both the governmental and nonprofit sectors. Police may not be provided with information about those prosecutions, although the information will be held in the relevant court system. In these cases, records held in the court system will not match records from the NPRS and local police systems.

The police systems automatically upload selected information to the national database in a system-to-system communication, through an XML schemer. A set of fields is populated with information pertaining to this record. It is a matter of state legislation as to what information is shared with the national system; however, rules around information provision are broadly similar

across the jurisdictions (see Section AUS 2.2 below). Only policing systems are linked to the national system, and uploading timelines range from instantaneous to overnight. The national data set is refreshed every day with the new data set transmitted by the various police jurisdictions, with records that have been changed locally identified and updated in the NPRS and new records added to it. The NPRS has no system-to-system link to corrections agencies and is not typically updated with information relating to corrections, such as release on parole.

AUS 2.2 Content

While state-level information systems hold a wealth of data about an individual's interactions with the criminal justice system, such as details of their involvement in an incident and criminal cases against them, ACIC's database is more strictly focused on criminal-history information. In practice, if an officer seeks more detailed information on a person of interest, they may contact directly the police force that maintains the relevant data.

Data held in ACIC's national system pertaining to a specific individual typically includes

- their name and other identity information, such as date of birth, place of birth, driver's license number, and passport number (if the individual is considered a flight risk)
- photographs of the individual and links to their biometric data in the National Criminal Investigation DNA Database (NCIDD) and NAFIS, where they exist
- warnings about the individual and outstanding warrants
- their offense history, including arrests and convictions and the jurisdiction(s) in which they occurred
- protection and violence orders relating to the individual
- firearm-related records, such as ownership or being found in illegal possession of a firearm
- information relating to records within the National Child Offender System (NCOS).

Records in the national system would not necessarily have details of probation or orders issued by courts, for example, to stop threats or acts of domestic violence, similar to a restraining order in the U.S. Furthermore, if there are multiple warrants outstanding for an individual, some states will provide only details of the highest-order warrant to the national database.

AUS 2.3 Data Retention

In Australia, the rules around the retention of criminal-history information are a matter of state rather than federal law: each state has established its own policies on how long it retains data generated by its own criminal justice system. In general, policing information relating to the fact of an interaction between police and a person of interest, any charges, and any subsequent conviction collected on policing systems is not routinely deleted by the police. However, there are exceptions to this rule. For example, AFP's policy is to retain all criminal-history records in its system pertaining to an individual until their 105th birthday, although no automatic alerts are triggered on the date to ensure compliance with this policy. There are also instances (e.g., during

the digitization of records in the 1990s) where decisions may have been made within the relevant jurisdiction not to upload older records into its electronic system. These records are not destroyed per se but are not readily accessible through the national system.

The royal prerogative of mercy (POM) may be used to pardon an individual convicted of an offense or to mitigate a sentence. Although this power is invested in the monarch, it is delegated to her representatives in Australia: for offenses against Commonwealth, Northern Territory, and Australian Capital Territory laws, the governor general; for state-level offenses, the relevant state governor. Governors act on the binding advice of the relevant attorney general in these matters. There is some variation between jurisdictions in how the POM operates. The information is retained but may not be disclosable in certain circumstances.

ACIC does not delete any records from any jurisdiction. However, the data held in the system are refreshed daily with updated files from across the jurisdictions, and there are no historical records of data sets previously held within the system. This means that if a record were changed or deleted by the jurisdiction that owned the data in its system, the national system would automatically be updated with the new information, and the previous content would be lost. In some police jurisdictions, records cannot be deleted in their local system, but the jurisdiction may ensure that a particular record is not accessible nationally through a search in the NPRS.

Retention of Biometric Information

ACIC also manages two national biometrics databases, NAFIS, operational since 1986, and NCIDD, operational since 2001. NAFIS is an automated fingerprint and palmprint database and matching system and is used by police agencies, as well as the Australian Department of Home Affairs. NAFIS allows users to upload and search fingerprint data. If a search of NAFIS results in a hit, the individual's CNI number is identified. The person conducting the search will then use the CNI number to look for the record in their local system first and, if there is no result, in the NPRS. The database holds fingerprint and palmprint images collected by police and immigration authorities, basic biographic information about the individual, and unidentified fingerprint and palmprint impressions recovered from crime scenes. While not every individual with a criminal-history record in the NPRS has a fingerprint record in NAFIS, every individual with a record in NAFIS has a record in the NPRS. NCIDD contains approximately 840,000 DNA profiles. Australian police forces use NCIDD to support criminal investigations and to assist in the identification of missing or deceased persons.

As with criminal-history records more generally, retention rules for biometric information are state based and depend on the legislation under which the biometric information was collected. For example, the retention of biometric data gathered in NSW as part of a criminal investigation is governed by the Crimes (Forensic Procedures) Act 2000 (NSW). The act provides for the destruction of forensic samples in the following circumstances:

- The person is acquitted of the charge.
- No conviction has been recorded in the matter.
- A conviction is overturned.
- The forensic sample was taken pursuant to an interim order (which can be imposed, for example, when an individual does not or cannot consent to a forensic procedure), if the order is disallowed by a magistrate.
- Criminal proceedings against the suspect have not been instituted within 12 months or have been discontinued. In certain circumstances, the 12-month period may be extended by a magistrate.

ACIC relies on police agencies to ensure that the data held in the national-level databases are in compliance with local laws around retention. States can delete their own records and can request that records be deleted in the NPRS. ACIC will act on the request if it was properly approved and only at their instruction.

AUS 2.4 Access to Data for Operational and Civil Purposes

Institutional Access for Operational Purposes

As noted above, the NPRS is used by law enforcement agencies across the country to share and access information on persons of interest and to facilitate criminal investigations. In addition, there is a small number of non-law-enforcement agencies that can access the NPRS directly. All access requires approval by the ACIC board and by all contributing jurisdictions, and applying agencies must satisfy the board that there is a legitimate reason to gain access and that they will comply with certain technical standards. These agencies' access to the NPRS is restricted to the information they need for their operations. ACIC has recently developed a limited-view functionality so that it is easier to facilitate access to some but not all records or parts of records for these agencies with access to the NPRS. Courts generally cannot access the NPRS or link to it directly, except for information that is held in the NPRS on domestic violence orders. Corrections agencies cannot access the NPRS or link to it directly. In general, any criminal-history information that courts and corrections agencies require for an individual is supplied by the local police force.

There is no direct access to the NPRS from outside of Australia. However, such agencies as Interpol, along with regional policing partners, may receive information from the NPRS in relation to criminal investigations or following a deportation order. Furthermore, some agencies may partner with state police agencies for investigations and be able to access information relating to the individuals involved; ACIC would not be aware of access by nonpolice users through local police agencies.

An officer conducting a search for an individual's record may search the NPRS, their local information system, or both simultaneously, with one set of results provided. Most typically, officers search both sets of data. In the past five years, ACIC has moved to change how data held in the NPRS is structured so that law enforcement officers may access the NPRS through a

variety of means. This may include access via such handheld devices as iPads, desktop computers, mobile data terminals in vehicles, or by radioing into a central operations room, depending on the jurisdiction's information technology resources. Most commonly, an officer would run a search using the individual's name and date of birth and biometric records, where they exist. The NPRS employs a wide name-matching algorithm to match the name entered into the search with the records it holds.

In practice, the most common use of the NPRS by officers is not to review criminal records. Rather, they rely on the system for any intelligence that may provide them with situational awareness when dealing with a person of interest, such as weapons warnings, and to check if the individual has any outstanding warrants. The NPRS is also used by law enforcement during criminal investigations—for example, for identification purposes.

Access to Criminal-History Data for Civilian Purposes

ACIC also provides NPCS, which facilitates criminal records checks for a variety of civilian purposes, including

- preemployment checks
- working with children or vulnerable groups
- licensing applications
- citizenship and visa applications
- adoption applications
- determining the suitability of an individual for jury duty.

An application for a police check may be submitted in one of two ways. First, an organization that has been accredited by ACIC and has undergone training administered by NPCS can request a police check on behalf of an individual. An organization is eligible to become accredited if it is an Australian registered business; can commit to submitting a minimum of 500 checks over a five-year period; agrees to be bound by the federal Privacy Act 1988 and Australian Privacy Principles (OAIC, n.d.); can implement the required security management measures to protect the individual's personal and police history information; and will dedicate personnel to the process. There are approximately 240 accredited organizations, comprising federal government agencies, private-sector businesses, and not-for-profits and screening units for working with children or vulnerable people. Second, an individual may request their own police check through their local police agency, which will provide the result to the individual.

An individual who is seeking to work or volunteer with children or vulnerable people is required to apply for a Working with Children Check. Each state and territory government has a dedicated screening unit that reviews any information held on an individual nationwide and issue relevant permits or registrations to work with such groups. In two police jurisdictions, this unit sits within the police, and in the remaining six, the unit sits within a government agency that is outside of law enforcement. No other organizations are permitted to conduct this kind of check.

If the applicant passes the check, they may be registered to work with children and/or vulnerable people for a set period. There is some variation across the jurisdictions in relation to who is required to be registered to work with children, the type of criminal or professional history that may prevent an individual from working with children, and for how long a registration is valid. A Working with Children Check may check other information systems beyond the NPRS, such as court databases, for prosecutions brought by nonpolice agencies, and professional malpractice record systems.

The police check involves processing an individual's biographic details (such as name and date of birth, not their biometric data) in a central index of names. A name-matching algorithm is used to determine if the individual's name matches any others with a criminal record across all Australian jurisdictions. Approximately 70 percent of checks have no matches and are completed in real time. The remaining 30 percent require further assessment by the jurisdiction(s) that owns potential match records. The check will be manually processed by police personnel in the relevant jurisdiction(s) to determine if their records match the identity of the individual requesting it.

If there is a match, the agency will then apply the disclosure laws and procedures that are applicable in that jurisdiction. This includes relevant information release policies, as well as the jurisdiction's "spent conviction"[4] legislation, under which certain offenses cannot be disclosed in NPCS checks if a certain amount of time has elapsed since the conviction was recorded. Each jurisdiction has its own legislation on which offenses may be spent and on the length of time required to exclude it from the check result. The results are then sent to the jurisdiction from where the check request originated, where that jurisdictions disclosure legislation is also applied. Any results of an NPCS check would therefore have to pass through the disclosure rules of the state where the offense occurred and the state where the request originated.

Two check results are possible:

- **No disclosable court outcomes.** An individual has no police history information or no information that can be released due to the category and purpose of the check.
- **Disclosable court outcomes.** There is police history information that can be released. Depending on the purpose and category of the check and relevant spent conviction legislation or information release policies, information disclosed on the check results report may include
  - charges
  - court convictions, including penalties and sentences
  - findings of guilt with no conviction
  - court appearances
  - good behavior bonds or other court orders
  - matters awaiting court hearing

[4] A spent conviction cannot be disclosed in certain circumstances, provided a specified period of good behavior has passed since the offense occurred.

- traffic offenses.

According to information from 2018, in the past financial year, ACIC facilitated over 5 million checks through the NPRS, raising about AUD $93 million in revenue for the organization. Police agencies receive a small fee from ACIC for their assistance in providing information when there is a match in their jurisdiction, provided the check application did not originate in their jurisdiction. ACIC funds all national-level police information systems, including the NPCS, the NPRS, the NAFIS, and the NCIDD.

AUS 3. Addressing Data Quality and Completeness

AUS 3.1 Procedures to Assess and Ensure Information Accuracy and Completeness

All Australian police forces are responsible for the quality of their own data; ACIC does not audit or change the data held on the national system. There is some variation across the police jurisdictions in how data accuracy and completeness are assessed and safeguarded. Police forces may dedicate officers to the task of ensuring that data entry is accurate, monitoring the use of the system, and auditing criminal records for errors. However, quality control processes in relation to ensuring accuracy varies by state.

AUS 3.2 Limitations of the Use of Data for Prosecution and Judicial Purposes

A number of issues with the quality and completeness of data held within the NPRS have been identified. First, the NPRS is only complete nationally from the early 1990s. Therefore, some criminal-history information for some individuals may be missing from the national system. In addition, at the point of creating a record for a person who has contact with the police, there is a risk that this record will not be linked to any existing records. This may occur if the individual is not fingerprinted for either this arrest or a previous arrest and the officer entering the individual's details into the local system is not aware that there is an existing record for that person. In such a case, a new, duplicate CNI number is created for the individual. Similarly, if there is an error with the CNI number (e.g., an incorrect digit is entered), a new record may be created and not linked to existing records. When conducting police checks, a wide naming algorithm is used to identify same or similar names, and unlinked records may be revealed as part of this process. In such cases, if the person conducting the search is satisfied that the records returned from the search pertain to the same individual, the searcher can initiate actions for the linking of the records. If the existing records are from another police jurisdiction(s), all relevant jurisdictions must engage with and agree to the linking of the records.

The absence of identity resolution to link multiple nominal records pertaining to the same individual poses some challenges particularly for police running an NPRS check in the field. An officer may receive multiple results from a search, some of which may relate to the same person. Where such a situation arises, the officer may have to ask the person about their criminal history

or contact the police force(s) that owns the record(s). In some police jurisdictions, police are provided with mobile devices that can take fingerprints and check them against NAFIS, and if there is a result against that individual, their CNI number is produced. The officer can then use the CNI number to search their local criminal-history database and/or the NPRS. However, as noted above, not all individuals with criminal-history records in the NPRS have fingerprints in NAFIS.

For an NPCS check, agents processing the application have more time and can refer matches to the relevant jurisdiction(s) to validate the identity of the individual. ACIC is currently working on a new information system that will improve identity resolution. However, the process is complex, and a key issue is the matter of data ownership. ACIC cannot link criminal records across police jurisdictions as that would entail changing state-owned data. Furthermore, as the national system is currently refreshed every day, the links made across jurisdictions would be lost by the next day.

With respect to the NPCS checks, the application of state and territory disclosure laws and regulations can occasionally lead to inconsistencies in the release of criminal-history information across jurisdictions. If an individual applies for a check within a particular jurisdiction, information may be released that would be withheld in another jurisdiction, and vice versa. This applies to spent convictions as well as certain kinds of offenses. For example, traffic offenses may be disclosed in checks in some states, but if an application is made in a state that does not disclose such offenses, this offense history will not be released. This has created concerns on the part of some stakeholders that individuals may exploit the system by applying for a check in a jurisdiction that will produce the most favorable results for them. This is made easier by the fact that an individual may apply online to an accredited organization that is based in another state and is bound by the information disclosure laws and regulations of that state.

Differences in criminal codes across the states also create issues in standardizing offenses. Some of these issues are easier to resolve than others. For example, in some states, breaking into and stealing from a house is called a “burglary and theft”; in others, it is called a “break, enter, and steal.” More complicated are differences in definition, such as what constitutes rape and/or sexual assault. In addition, there are some offenses that exist in some states but are decriminalized or legal in others, such as low-level drug possession or prostitution.

Some issues with court data have been identified. On occasion, police forces do not receive complete or accurate information relating to a court outcome or are not provided with information relating to further sentencing, appeals, or any other decisions made subsequent to the initial outcome. This has been linked to human error when prosecutors manually update the court system, for example, by using the incorrect form. When errors such as these come to the attention of officers managing the local information systems, they are immediately corrected. However, this typically occurs on a case-by-case basis. Concerns have also been raised about the timeliness of court updates in some cases, particularly when there are no direct links between court and police information systems or when connectivity to courts in remote areas is

problematic. This kind of delay may pose public and police safety risks. For example, when a domestic violence victim is granted a protective order against their attacker, they are statistically at highest risk of further violence in the days immediately after the order is made. If a police force is not updated with information relating to the order in a timely fashion, it may not be properly equipped to protect the victim during this time. However, most courts in Australia have electronic links to police information systems or are currently in the process of establishing such links.

AUS 4. How Are Data Used for Research Purposes?

Historically, criminal-history information held in the national system has not been made available for research purposes. The use of these data for research would require the agreement of all participating police agencies, making nationwide research projects difficult to initiate. However, in 2015, staff from the AIC, the national crime and justice research center, were transferred into ACIC under a Machinery of Government process and then temporarily assigned back to the AIC. Although the AIC remains an independent entity and holds data separately from other parts of ACIC, AIC researchers have had a level of access to NPRS data since late 2017.

The AIC requested and was given access to a small data set from the NPRS for a research project on organized crime offenders. These data pertained to the criminal history of approximately 7,000 organized crime offenders, with all contacts between the individual and the police, including in relation to offenses for which they may not have ultimately been convicted. The process of gaining access to this data set was complex, as the legislation under which ACIC operates is onerous, and data-sharing arrangements must meet strict requirements. One central concern was that if individuals in the data set could be identified by researchers, this could amount to disclosures of spent convictions, which would violate state and territory laws. To overcome this issue, the data set was anonymized, and only six variables were included in the shared data set: each individual's date of birth and gender, the year(s) of the individual's offense(s), offense type, process classification, and the year the individual was added to the National Criminal Target List (another database maintained by ACIC, which holds information on nationally important serious and organized crime targets). Subsequently, another variable was added: whether the individual was identified as a member of an outlaw motorcycle gang. With the approval of the AIC human research ethics committee, the AIC used the data to create a criminal careers database and analyze it for specific research activities.

This data set was up-to-date at the time of sharing but has not been refreshed since; this would require an additional request for records created since the data set was shared. There is no time limit on how long the AIC can retain these data, and in terms of data security, the AIC follows the normal protocol for the holding of data provided by another criminal justice agency. This protocol requires that the data are held on the AIC secure server, completely deidentified,

and transmitted appropriately (e.g., with password protection) and that results of the research are reported in aggregate format.

A small number of issues have been identified in relation to using the NPRS data for research. First, the NPRS is only complete nationally from the early 1990s. Therefore, some information relating to the criminal careers of the individual in the AIC data set may be missing. In addition, as noted above in Section AUS 3.2, information in the NPRS relating to court outcomes may occasionally be incomplete or inaccurate.

In terms of future avenues of research using NPRS data, the AIC is currently pursuing proposals on domestic violence offending research using information held in the NPRS on protection orders. The AIC also has a large number of other research projects using criminal-history data sourced directly from states and territories. Furthermore, a number of state governments have created research agencies that use data from their local police information system. In some cases, they also provide access to their locally held data to external researchers. State-level research is discussed in AUS Appendix A.

3. Canada

Key Findings

- The Canadian Police Information Centre (CPIC) is the country's national communication system that provides public safety and criminal justice information. In addition to other data banks, it provides access to the National Repository of Criminal Records (NRCR).
- The NRCR is managed by the Royal Canadian Mounted Police (RCMP).
- NRCR criminal-history data include convictions and nonconvictions. All criminal record information is managed according to Canadian legislation. Retention of data is dependent on the court disposition received and type of offense. Retention rules differ for youth criminal records.
- Criminal-history data are provided electronically to the RCMP in a standardized format by local police agencies. Apart from serious youth offenses, there is no legislation that mandates the requirement to submit criminal record information to be added to the NRCR. However, all agencies voluntarily submit criminal record information to the RCMP, as they are the stewards of the NRCR.
- The NRCR is a fingerprint-based criminal-history record database, that includes fingerprint information collected by the arresting agency in accordance with the Canadian Identification of Criminals Act.
- Access to NRCR data is granted to over 3,000 user agencies, consisting of criminal justice agencies and other public authorities. Private individuals typically obtain information from the NRCR via a criminal background check.
- There are delays before some information is uploaded onto the NRCR. This means that an individual's criminal history may temporarily be inaccessible unless local agency records are also searched. The RCMP has been engaged in long-term efforts to address the situation. The RCMP has continued to work on the Criminal Justice Information Management (CJIM) project to improve the quality and timeliness of criminal record information submitted from law enforcement agencies. CJIM allows police services to use a standardized process to electronically report criminal disposition information to the NRCR in virtually real time, replacing the older paper-based process.
- Robust information systems exist at the subfederal level as well. Each province has its corrections database, and provinces also operate law enforcement record management systems. Both types of systems can be used for operational and research purposes alike.
- Provincial law enforcement databases draw data from local police forces and may include information on individuals who have been in contact with law enforcement but do not have any criminal record. Local and provincial databases may also have different (and inconsistent) data retention rules. For these reasons, local and provincial databases may hold data that are not available in the NRCR.
- There is relatively little criminal justice research conducted using NRCR data, and, while possible, obtaining direct access to the data is considered difficult for researchers.
- Data held by local and provincial agencies frequently serve as a primary data source for researchers because the agencies are the original sources of the data held in the NRCR. Therefore, they hold the same data as the NRCR and in addition may have data that were not reported (or yet uploaded) to the NRCR.
- Research collaborations with local and provincial agencies are governed by their own policies and procedures, which vary across individual jurisdictions. There is no national standard for research collaborations involving access to data via local agencies.

CAN 1. Overview of the Country and Criminal Justice System

CAN 1.1 Political and Constitutional System

Canada is a constitutional monarchy with a population of over 36 million.[5] It is a federal country consisting of ten provinces and three territories. Accordingly, legislative powers are shared between the federal and provincial governments. Areas of competence reserved for the federal government revolve around matters of national interest, such as international and interprovincial trade regulation, national defense, and citizenship. By contrast, provincial governments have responsibility for issues of more local character, such as education, health care, and natural resources. In addition, some powers are constitutionally envisaged to be shared between the federal government and the provinces; these include immigration and agriculture (Field, 1992; Government of Canada, n.d.). Territorial governments have similar responsibilities as provinces, although their powers are not derived directly from the constitution but rather from the federal government (Cameron and Simeon, 2002; Yukon Legislative Assembly, 2012). In two other notable differences from provinces, territories do not own their land (it remains the possession of the federal government) and their constitutions need to be amended via federal legislation (Legislative Assembly of the Northwest Territories, n.d.).

CAN 1.2 Criminal Code and Procedure

The Canadian Parliament has exclusive authority over criminal procedure, and, correspondingly, there is only one criminal code in Canada.[6] However, federal, provincial, and territorial governments all share responsibilities for the administration of justice in the country. As a result, criminal justice agencies exist at all levels of government.

There are three types of offenses in the Canadian Criminal Code. Summary offenses are relatively minor cases and typically are heard in a provincial court. The maximum penalties for summary offenses are fines (not more than CAD $5,000) or a short custodial sentence (not longer than six months).[7] *Indictable offenses* represent more serious cases and are heard in a provincial or superior court either by a judge alone or by a judge and a jury (Department of Justice, 2017a). Finally, *hybrid offenses* can be treated as either summary or indictable, with the decision on how to proceed made by a prosecutor.

In addition to offenses against the Canadian Criminal Code, individuals may be found guilty of provincial offenses. Provincial offenses are minor infractions governed by the Provincial Offences Act and any statutes enacted by the provinces. Examples include traffic violations and infractions in such areas as liquor licensing or occupational health and safety. They are not related to the Canadian Criminal Code and are typically resolved with a fine.

---

[5] 2017 data (Statistics Canada, 2018).

[6] Civil procedure is organized by the provinces/territories (Department of Justice, 2017a).

[7] According to Article 787 of the Criminal Code.

CAN 1.3 Court Dispositions and Penal Sanctions

There are several ways in which criminal charges can be resolved in courts in Canada. In fiscal year (FY) 2015, about two-thirds of adjudicated adult cases (63 percent) resulted in a finding of guilt (Maxwell, 2017). Probation is the most common sentence for defendants who are found guilty, accounting for 43 percent of sentences in FY 2015, followed by custodial sentences (37 percent). Of defendants sentenced to custody, the vast majority (88 percent) received a sentence of fewer than six months (Maxwell, 2017).

A finding of guilt can also result in a discharge. Two types of discharges, meaning situations where there is a finding of guilt but no conviction imposed, exist in Canada:

- absolute (no conditions attached)
- conditional (with probation orders).

Additional court outcomes include a withdrawal of charges[8] (21 percent of cases in FY 2015), a stay of charges (11 percent),[9] acquittal (4 percent), and other types of decisions (1 percent), such as a finding of not guilty on the grounds of mental disorder (Maxwell, 2017).

CAN 1.4 Criminal Justice Agencies

Law enforcement: Law enforcement agencies in Canada exist at three levels of government—federal, provincial/territorial, and local/municipal. Policing at the federal level is the responsibility of the RCMP. In addition, the RCMP is contracted to provide policing services at the provincial/territorial level for eight provinces and all three territories, as well as in over 150 municipal jurisdictions, 600 indigenous communities, and a small number of international airports (RCMP, 2018a). Only three provinces do not contract policing services fully to the RCMP. Ontario and Quebec have their own provincial police forces—the Ontario Provincial Police (OPP) and Sûreté du Québec (SQ), respectively. In the province of Newfoundland and Labrador, the RCMP operates alongside the Royal Newfoundland Constabulary (RNC)—the RNC polices a small number of larger population centers, while the RCMP provides services in the rest of the province (Alain, Corrado, and Reid, 2016). As of 2017, there were 141 stand-alone municipal jurisdictions and 36 First Nations jurisdictions that administered their own police services and did not contract with the RCMP (Conor, 2018). These include the largest Canadian cities—all three most populous cities (Toronto, Montreal, and Vancouver) have their own municipal police forces. In total, in 2017, there were nearly 70,000 sworn officers in Canada, amounting to a rate of 188 officers per 100,000 population (Conor, 2018).

---

[8] For example, after diversion to an alternative measure.

[9] Similar to a withdrawal of charges, the prosecution is discontinued. However, the proceedings may be recommenced within a certain period (typically a year). If the prosecution is not restarted, it is considered to have never started (i.e., the individual may be charged again).

Prosecution: The vast majority of criminal cases in Canada are prosecuted by Crown attorneys (also called Crown counsel or Crown prosecutors in some provinces) who are responsible for criminal cases at the provincial level. They make the ultimate decision whether charges, typically laid down by the police, will be prosecuted in court and will formally oversee any potential prosecution. They may also provide legal advice to the police during investigations, which are formally led by the law enforcement agency.[10] Crown attorneys, appointed by the provincial public prosecution services, report in each province to the provincial minister of justice (also called attorney general in some provinces).

The responsibility to prosecute federal cases lies with the Public Prosecution Service of Canada (PPSC).[11] Such cases include Criminal Code offenses committed in the territories and offenses against other federal statutes in such areas as organized crime, terrorism, and taxation (PPSC, 2018).

Courts: The court structure in Canada is similar across all provinces. The vast majority (greater than 99 percent) of criminal cases are heard by lower provincial (and territorial) courts.[12] Higher provincial courts are called superior courts. They serve as trial courts for the most serious criminal cases and as appellate courts for cases heard at the provincial courts. Provincial court judges are appointed by the provincial governments, and superior court judges are appointed by the federal government.[13] At the federal level, the Supreme Court of Canada hears appeals from provincial appellate courts and decides on constitutional matters.[14]

Corrections: In Canada, there is one federal corrections agency (Correctional Service of Canada [CSC]), as well as one corrections agency in each province/territory, with a clear division of responsibilities between the two levels of government. The CSC is responsible for the housing and supervision of offenders sentenced to custody for two years or more (federal offenders) and for the supervision of parolees released from all correctional facilities (CSC, 2016). CSC, however, does not make decisions on prisoners' conditional release: that is a responsibility of the Parole Board of Canada (PBC). Provinces and territories are in turn responsible for the housing and supervision of offenders sentenced to custody for fewer than two years and for the supervision of individuals who received noncustodial community and

---

[10] See, for example, Alberta Justice and Solicitor General (n.d.).

[11] The PPSC duties are carried out by its prosecutors appointed by the director of the PPSC as well as private-sector lawyers retained as agents. See Parliament of Canada (2006).

[12] Data from 2014/15 (Maxwell, 2017).

[13] The appointment of provincial court judges is made by the provincial lieutenant governor, based on the advice from the cabinet, which in turn is informed by recommendations from the provincial minister of justice. The appointment of superior court judges is made by the governor general, based on the advice from the cabinet, which in turn is informed by recommendations from the minister of justice.

[14] In addition, there are three federal courts with specialized noncriminal jurisdiction: the federal court hears cases in such areas as intellectual property and federal-provincial litigation; the tax court hears appeals to tax assessments; and the federal court of appeals hears appeals from these two courts (Department of Justice, 2017a).

alternative sentences. In addition, pretrial detention and, in accordance with the Youth Criminal Justice Act, youth supervision (in all forms) are also the responsibility of provinces/territories.

During FY 2015, 3 percent of all adults sentenced to custody in criminal cases received a sentence of two years or more and were under CSC supervision (Maxwell, 2017).[15] Among adults under provincial and territorial supervision, a large majority (79 percent) were serving a noncustodial sentence and were under supervision in the community, with the remaining 20 percent held in custody.[16] In FY 2017, federal offenders represented 36 percent of all adults in custody (Malakieh, 2018).

CAN 1.5 Size of Criminal Justice System

Excluding traffic offenses, there were over 1.9 million reported violations of the Criminal Code in Canada in 2017. This corresponds to a police-reported crime rate of 53 incidents per 1,000 population (Allen, 2018). Violent crimes accounted for approximately one-fifth of all police-reported offenses in 2017 (Allen, 2018).

In FY 2015, adult criminal courts in Canada adjudicated nearly 330,000 cases involving almost a million criminal charges. As discussed above, slightly over 200,000 cases (63 percent) resulted in a finding of guilt (Maxwell, 2017).

The number of incarcerated adults in Canada on a typical day in FY 2017 was slightly below 40,000 people, with an adult incarceration rate of 136 inmates per 100,000 population (87 in provinces/territories and 49 in federal facilities) (Malakieh, 2018). The number of inmates is lower than the number of annual custodial sentences because a large proportion of these are relatively short—for instance, in FY 2015 more than half of received sentences were one month or less (Maxwell, 2017). In FY 2017, roughly 60 percent of adults held at provincial and territorial detention facilities were remand (pretrial) prisoners (Malakieh, 2018).[17] As a proportion of the total prison population, including federal inmates, the share of remand prisoners in FY 2017 was 37 percent (Malakieh, 2018).

[15] The fiscal year for the Canadian federal and provincial governments runs from April 1 to March 31 (i.e., FY 2015 ran from April 1, 2014, to March 31, 2015).

[16] Data from 2016/17 (Malakieh, 2018).

[17] Due to unavailable data, this statistic excludes custody rate information from Alberta.

CAN 2. Canadian Police Information Centre

CAN 2.1 History and Content

The national-level criminal-history information system in Canada is the NRCR, which may be queried through CPIC, both of which are maintained and operated by the RCMP. The origins of the NRCR trace back to the 1898 Identification of Criminals Act, which provided for the fingerprinting of individuals charged with indictable offenses (Kilgour, 2013). To manage the collected fingerprints and associated criminal records, the act also established a central agency in Ottawa, to which local police agencies would send their fingerprints. The objective of this arrangement was to aggregate all criminal records in Canada under the purview of this central bureau. In 1920, the ownership of this criminal record system passed onto the RCMP. The sharing of law enforcement information was the basis for CPIC, which was formally established in 1972 (Kilgour, 2013). In 1973, the RCMP introduced an electronic digital system, which enabled fingerprints and associated criminal-history information to be retrieved electronically by authorized users. Today, CPIC is a centralized computer system that is used for the storage, retrieval, and sharing of information maintained by the originating agency and consisting of four data banks (summarized in Table 3.1).

Table 3.1. Canadian Police Information Centre Data Banks

Data Bank	Content	Data Provided By	Entries Managed By
NRCR (Identification Data Bank)	Biographic information, charges, and court dispositions	Local police agencies	RCMP (Canadian Criminal Real Time Identification Services [CCRTIS])
Ancillary Data Bank	Vehicle registration, driver's licenses, wandering persons, Interpol, and penitentiary inmates[a]	Originating agencies (e.g., CSC, provincial Registry of Motor Vehicles, or Alzheimer Society)[b]	Originating agencies
Intelligence Data Bank	Criminal intelligence information (e.g., personal information on individuals implicated in investigations of serious and organized crime)	Criminal intelligence agencies	Criminal intelligence agencies
Investigative Data Bank	Information pertaining to criminal investigations (vehicles, property and marine; persons, accused, court action, missing, parolee, and wanted)	Investigating agencies	Investigating agencies

[a] "Wandering persons" is a register of people who have been reported as at risk of going missing; for example, people living with dementia. The objective of collecting this information is to help ensure the individual in question is promptly identified and reunited with his or her caregiver.
[b] Department of Justice (2016).

As of 2016, the NRCR contained approximately 4.25 million criminal records (Senate of Canada, 2016). The repository is maintained by the RCMP's CCRTIS and stores three types of information:

- biographic information (names and aliases, date and place of birth, sex, address, and physical descriptors)
- information on charges
- information on court dispositions.

Information on criminal history is reported by local police to the RCMP, with each file including fingerprint information.[18] The local police force submits the information electronically to the RCMP, using standardized forms and electronic capture devices.[19] The information is transferred in the form of electronic packets compliant with standards of the National Institute of Standards and Technology to CCRTIS, which then uploads the data into the NRCR. To make a submission to the NRCR, there are mandatory fields that must be reported. CCRTIS is the only entity with the authority to make or modify entries in the NRCR, although the originating agency edits data in the other three CPIC data banks where appropriate (RCMP, 2014b). There are no formal requirements on when local police forces should initiate the transfer process; they start the transfer as soon as it is practical for the agency to do so. The submitted records are continually updated as new information is collected. The information is entered in the repository in the language (i.e., English or French) used by the submitting agency.

By law, local police forces are required to report only information on juvenile (ages 12 to 17 years old) indictable and hybrid convictions. There are no formal reporting requirements at all with respect to information on adults, although, in practice, agencies do voluntarily report large volumes of criminal record data to the RCMP.[20] As will be discussed later in this chapter, this arrangement has implications in a range of areas, including data protection and data completeness. This discretion afforded to local agencies manifests itself primarily in the following two areas:

- **Types of offenses.** Typically, only information on indictable and hybrid offenses is collected on the NRCR. This is because the NRCR is a fingerprint-based information system and, in accordance with the Identification of Criminals Act, fingerprints can be obtained only in connection with these two types of offenses. However, local police services have the option to report information on summary offenses, such as when they are connected to an indictable offense and the local police feel it would be beneficial for

[18] In a very small number of cases, the quality of the fingerprint is not sufficiently high to add to the file.

[19] The options for electronic transfer are live scan or card scan (for situations where prints were taken by the ink-and-roll method and then converted to an electronic format).

[20] Section 115(2) of the Youth Criminal Records Act says that police forces "may" provide the information when the individual is charged and "shall" provide the information when the individual is convicted. With respect to adults, the Identification Criminal Act provides for the possibility to transfer data to the RCMP; however, strictly speaking, this remains optional.

the NRCR to contain the record. Information on provincial offenses is not recorded (RCMP, 2014b).

- **Types of court dispositions.** The NRCR contains information on dispositions that involve a finding of guilt (i.e., convictions and discharges). In addition, local police agencies have discretion over what nonconviction information (e.g., information on charges resulting in acquittals) is reported to the NRCR (CCLA, 2014).

Biometric Data

As noted above, the NRCR is fingerprint based, and individual files are organized (and can be queried) on the basis of sequential fingerprint serial numbers (FPS). No other biometric information is currently being stored on the NRCR, although (as discussed below) some searches of the NRCR will indicate that a person has a record in the National DNA Data Bank. In 2016, the RCMP announced plans to introduce photos into the CPIC system (RCMP, 2016b).

CAN 2.2 Data Retention

The retention of criminal-history data held by the NRCR depends on the type of court disposition and whether the offender is an adult or a juvenile (ages 12 to 17 years old).[21] The summary of key information is presented in Table 3.2; we then discuss the retention rules applicable to all three possible court dispositions (convictions, discharges, and nonconvictions).

Table 3.2. Overview of Data Retention Arrangements per Disposition Type in Canada

Disposition Type	Adults	Youths
Convictions	Retained until the individual is 125 years of age. Record can be sequestered if the RCMP is notified that a record suspension has been ordered.	Summary: sequestered after 3 years after completion of sentence. Indictable: sequestered after 5 years after completion of sentence.
Discharges	Absolute: retained 1 year. Conditional: retained 3 years.	Same retention periods as adult discharge records, after which records sequestered.
Nonconvictions	No formal retention rules; data not automatically deleted. Application for file destruction can be filed with arresting agency, which will notify the RCMP.	Restorative and extrajudicial measures: automatic deletion. Other outcomes: sequestered.

NOTES: Relevant underlying legislation: Criminal Records Act and the Youth Criminal Justice Act. Table 3.2 provides information pertaining to discharges received on or after July 24, 1992. Older discharges are removed upon request.

Convictions

Adults: Criminal-history data on adults with convictions are held until they reach 125 years of age or until notification of their death (RCMP, 2018b). However, individuals may apply for a

[21] In accordance with the Youth Criminal Justice Act.

record suspension, which, if granted, means the record is sequestered from active NRCR files (although not destroyed) and will not appear in any searches of the system.[22] In practice, the outcome is as if the record had never existed in the first place.[23] However, as discussed below, the sequestered information can be reactivated if further criminal activity is recorded for the individual in question.

The application for the record suspension is made with the PBC, and individuals are eligible to apply after a waiting period following the completion of their sentence. The waiting period depends on the type of offense. For summary offenses, it is five years after sentence completion. For indictable offenses, the waiting period is ten years after sentence completion (PBC, 2018). Individuals with multiple offenses are eligible to apply for a suspension of all their criminal records at the end of all waiting periods for all their offenses. Two groups are not eligible for record suspensions at all: persons with more than three convictions for indictable offenses and persons convicted for sexual offenses against a child. For other sexual offenders, a record suspension can be granted, but the NRCR will retain a flag indicating the receipt of a suspension. The reason for this arrangement is the need to preserve the information for vulnerable-sector checks (see Section CAN 2.3).

As mentioned above, a suspension can be revoked in the event of a new offense, if the person is no longer of good conduct, or if they are found to have been ineligible or have lied on the application. If a suspension is revoked, the original criminal record is reactivated in the NRCR (PBC, 2019).

Since 1970, the PBC has granted more than 500,000 suspensions, 95 percent of which have remained in place (i.e., have not been revoked) (PBC, 2016b). In 2015 and 2016 alone, the PBC received over 12,000 applications for suspensions, of which almost 9,000 were accepted for processing.[24] Of these, 43 percent of applications were made in relation to an indictable offense. The vast majority of applications (95 percent) were approved. The most frequent offenses covered by these suspensions were driving under the influence of alcohol, impaired driving, assault, and drug-related crimes.[25]

Young persons: Records of summary convictions are available from the NRCR for three years after sentence completion. For indictable convictions, the record is visible for five years

---

[22] Deletion of a criminal record may also be authorized by a royal prerogative of mercy (i.e., clemency), which can revoke the individual's conviction and sentence. However, these cases are extremely rare and reserved for exceptional situations. To illustrate, between 2011 and 2015, only 14 requests for clemency were granted (PBC, 2016b).

[23] As discussed later, an exception to this are suspended records associated with sexually based offenses, which will be searched (and visible) for the purposes of a vulnerable-sector verification.

[24] The reasons for rejecting an application include ineligibility, wrong/missing information and documentation, and missing/incorrect fee. The number of applications for suspensions fell sharply following the reform of the Criminal Records Act in 2012, which made it harder to apply (PBC, 2016a).

[25] Specifically, breach of the Narcotic Control Act and breach of the Controlled Drugs and Substances Act (PBC, 2016a).

after sentence completion. After the expiration of these periods, the conviction is sequestered from active records (i.e., archived) so that it is no longer active or visible on NRCR searches.[26] If the young person is convicted of a new offense during the period in which the record is active (i.e., visible), the retention period is restarted. The sequestration of all records takes place after the expiration of the retention period associated with the new, latest offense. As with an adult record with a suspension, a sequestered youth record of an indictable offense conviction can be reactivated in the event of new criminal activity, although only if the new conviction occurs within a specified time frame.[27]

Discharges

Adults: The rules for data retention in relation to discharges depend on the type of discharge. For absolute discharges, the information is either deleted or sequestered one year after sentencing.[28] Records of conditional discharges are deleted or sequestered three years after sentencing.[29] If the discharge is the only information on record, the file is sequestered; if the record has additional information, the discharge will be deleted.

Young persons: The retention periods for juveniles are the same as for adults.[30]

Nonconvictions

Adults: There are no formal NRCR rules for the retention of nonconviction data on adults (e.g., information on charges resulting in acquittals) as there is no existing legislation addressing nonconviction information. Such data are not automatically removed from the system, and the only way for them to be deleted is for the individual to file an application for their destruction. This application needs to be sent to the arresting local police agency, which is the owner of the nonconviction information and will consider the request. If the application is approved, the agency will forward its decision to the RCMP, which will then delete the record in question. However, there are several grounds on which the RCMP may refuse to delete a nonconviction record. These include the existence of a conviction record or outstanding charges pertaining to the applicant. In addition, the RCMP will automatically reject any application and retain a

---

[26] The sequestered information continues to be available to law enforcement for the purposes of crime scene matching (per Section 128 of the Youth Criminal Justice Act). The record also continues to be available for a limited period for the purposes of the identification of a dead body or a person with amnesia (per Section 120 of the Youth Criminal Justice Act).

[27] Per Article 120 of the Youth Criminal Justice Act, this period lasts five years after the record's sequestration, unless it is a record of a serious violent offense for which prosecution sought an adult sentence, in which case the period during which a record can be reactivated is unlimited.

[28] Unless the discharge was received before July 24, 1992, in which case the removal can happen only on written request from the person concerned (RCMP, 2018b).

[29] Unless the discharge was received before July 24, 1992, in which case the removal can happen only on written request from the person concerned (RCMP, 2018b).

[30] As with conviction data, the sequestered records continue to be available for the purposes of crime scene matching and the identification of a dead body or a person with amnesia.

nonconviction record for a minimum of five years if the underlying charge is related to any of the following offenses: high treason or treason, potential terrorist activity, first- and second-degree murder, manslaughter, aggravated assault, and sexually based offenses (RCMP, 2014a). The nonconviction record will also be retained for a minimum of five years in cases where an individual has been found not criminally responsible due to a mental disorder.

Each police agency has its own rules and procedures for deletion applications. According to a 2014 analysis, nonconviction data are held on over 420,000 individuals in Canada (Cribb and Rankin, 2014).

Young persons: Retention of data on youths depends on the type of nonconviction. Information on charges resulting in restorative justice measures and extrajudicial measures (i.e., nonsanctions) are immediately deleted. Data on situations with other outcomes (e.g., charge withdrawals or peace bonds) are sequestered.[31]

Importantly, retention arrangements for both adults and young persons apply only to data held in the NRCR or at an RCMP agency. Local non-RCMP agencies, which are the owners of the data, have their own rules for data retention. In this regard, there is no common data retention standard and actual practices among agencies vary. Some agencies may hold information on their systems longer than a record is active on the NRCR.[32] This includes agencies that did not create the data but accessed them through the NRCR and may have copied the data onto their databases).

CAN 2.3 Access to Canadian Police Information Centre Data for Operational and Civilian Purposes

Access for Operational Purposes

Access to CPIC is granted to designated "CPIC agencies." As of December 2016, there were nearly 3,200 agencies with more than 80,000 users who have been granted access to CPIC. These agencies include Canadian law enforcement agencies, federal and provincial agencies with limited law enforcement power (e.g., Canada Border Services Agency, Correctional Service Canada, National Parole Board, Citizenship and Immigration Canada, and Canada Revenue Agency), and agencies with roles that support law enforcement (e.g., Transport Canada and Passport Canada) (British Columbia Civil Liberties Association, 2015; Department of Justice, 2016). Access is also granted to international partner agencies, including Interpol (IRC, 2016). U.S. agencies with access to CPIC are at both the federal (e.g., U.S. Customs and Border

[31] As with conviction data, the sequestered records continue to be available for the purposes of crime scene matching and the identification of a dead body or a person with amnesia.

[32] One practical manifestation of this issue is the occasional issue Canadians encounter when trying to enter the U.S. U.S. Customs and Border Protection is one of the CPIC user agencies, but there is no information on how many records may have been copied onto their databases. Records that have been copied to the U.S. Customs and Border Patrol's systems can be expected to be held irrespective of the RCMP's arrangements (CCLA, 2014).

Protection and the FBI) (RCMP, 2014b) and the state level (e.g., participants in Michigan's Law Enforcement Information Network) (LEIN, 2015).

To gain access to CPIC data, agencies need to complete a memorandum of understanding with the RCMP to govern their use of CPIC. These arrangements may differ depending on the type of user agency but invariably follow the RCMP's policies and procedures as laid out in the CPIC policy manual. Level of access to CPIC data afforded to individual agencies is controlled by the RCMP in accordance with the mandate of the agency (OPC, 2011) and is based on approval from the director general of the CPI Centre. Importantly, user agencies have the right to only query the NRCR through CPIC; they are not authorized to add, modify, or delete existing criminal-history records using the CPIC system (Kilgour, 2013). In addition, access to and use of CPIC is tracked and resulting metadata are stored by the RCMP (Kilgour, 2013). The RCMP also offers user agencies a course on how to query the database (CPIC Query Course) and a course on adding, modifying, and removing records from the Investigative and Intelligence Data Banks (CPIC Maintenance Course).

In undertaking searches of the NRCR for operational purposes, user agencies can access three layers of data, depending on what query they decide to run:

1. **CRII (Full Criminal Record):** This is the most complete set of information and includes the following data: individual's conviction history (exact information on charges, dates and details of convictions, and conditional and absolute discharges) and available related information provided by the police. This set of data is accessed with a CR (criminal record) query based on the FPS. The FPS is a sequential number that is assigned to a newly acquired set of fingerprints that have not been previously filed in relation to a criminal offense.[33] The level of CRII information that is accessible by CPIC users depends on their profile.
2. **CRS (Criminal Record Synopsis):** This is a summary version of information held by CPIC. The data obtained from the CRS are biographic information (sex, age, date of birth, eye color, height, weight, body marks, and known names and aliases), as well as broad categories of criminal offenses and any warning if the individual is considered dangerous (either to themselves or to others).
3. **CNI (Criminal Name Index):** This data set, intended for a rapid search, is a list of names of individuals for whom there may be an existing criminal record in the repository. It can be queried with a name-based (CNI) query, which will retrieve the FPS number, which can be subsequently used for further queries.

In addition to either FPS-based or name-based queries, information can be obtained with the submission of fingerprints to determine an individual's identity and criminal record.

[33] When the arresting agency creates a fingerprint record, it runs a search in the Automated Fingerprint Identification System (AFIS). If there is a match to an already existing fingerprint, the agency is notified of its number and the name of the individual. If there is no match, a new FPS is generated and assigned to the new fingerprint.

Access for Civilian Purposes

Civilian Criminal-History Checks

Information held by CPIC is also routinely used for the purpose of civilian criminal-history checks, such as for employment. Multiple modalities of these checks exist, depending on the purpose, breadth, and form of the check. Applications for a criminal-history check can be processed by third-party for-profit agencies; however, all searches of CPIC must be done by a certified CPIC user agency, even those done on behalf of third-party agencies (OPC, 2011). A civilian criminal-history check may be conducted only with the consent of the individual subject of the check.

Civilian criminal checks can be undertaken using the individual's name and date of birth or using fingerprints provided by the applicant.[34] Only fingerprint-based checks can confirm the existence of a criminal record and result in a certified product (see below). Name-based checks are done primarily as a means to ascertain whether a criminal record for an individual may exist and whether a fingerprint-based verification may be necessary. A name-based query can result in three types of responses:

- **Negative:** This is a confirmation that the combination of a name and date of birth did not identify any corresponding records.[35]
- **Incomplete:** This means that a search on the basis of the name and date of birth could not be completed. This response would be provided in situations where a search identifies a record that may be associated with the applicant but does not completely match the information provided by the applicant. This situation may be resolved by submitting a fingerprint-based application.
- **Positive:** This means that there is a *possible match* between the name / date of birth and an existing record in the NRCR. However, for this to be confirmed, a fingerprint-based search must be undertaken.

There are two types of verifications that can be run using CPIC data, depending on the desired depth of the search: criminal record verification and vulnerable-sector verification.

Criminal record verification is a query of the active files in the NRCR to check for (if name based) or confirm (if fingerprint based) the existence of a criminal record. A fingerprint-based version of this verification will result in a Certified Criminal Record product.

Vulnerable-sector verification is a more thorough search, typically undertaken in connection with work or volunteering positions within the vulnerable persons sector (CCLA, 2014). In addition to active NRCR records, this query searches criminal files in the NRCR with

[34] Unless noted otherwise, this section is based on the RCMP's "Dissemination of Criminal Record Information Policy" (RCMP, 2014b).

[35] According to the RCMP's dissemination policy, a CPIC agency may provide a negative answer if the query identified only nonconviction records and/or only youth records. To send out a negative response for a vulnerable-sector verification, reporting criteria must not be met for "Flagged Pardoned Sex Offender Records."

record suspensions associated with sexual offenses.[36] CPIC searches will also include its Investigative Data Bank and Intelligence Data Bank. In addition to CPIC searches, this verification will include a search of local police records in the jurisdiction where the applicant currently resides. All of these searches must be done by a CPIC agency that has jurisdiction in the place of the applicant's residence. The reason for this is that, as discussed in Section CAN 2.1, not all offenses get reported to the NRCR and local police records may hold information that is not available on CPIC. A fingerprint-based version of this verification will result in a Certified Vulnerable Sector product, which (with the applicant's consent) will be sent directly to the vulnerable-sector organization that required the applicant to undergo the check.

The various types of certifications and checks and their combinations are summarized in Table 3.3.

Table 3.3. Overview of Civilian Criminal Record Checks in Canada

Type of Record Check	Data Searched	Final Result
Name-based criminal record verification	NRCR active files	One of three standard responses: negative, incomplete, or positive (i.e., possible match)
Fingerprint-based criminal record verification	NRCR active files	Certified Criminal Record product
Name-based vulnerable-sector verification	NRCR active files NRCR suspended files associated with sexual offenses CPIC Investigative and Intelligence Data Banks Local police records	One of three standard responses: negative, incomplete, or positive (i.e., possible match)
Fingerprint-based vulnerable-sector verification	NRCR active files NRCR suspended files associated with sexual offenses CPIC Investigation and Intelligence Data Banks Local police records	Certified Vulnerable Record product

Canadian Firearms Program

CPIC data are automatically checked on a daily basis by the Canadian Firearms Information System (CFIS)[37] for the existence of a reported event involving a holder of a firearms license. If there is a match, the information is forwarded to the relevant provincial firearms office that may review the license in question. Conversely, CPIC provides access to the Canadian Firearms Registry On-line (CFRO), a subset of CFIS, by law enforcement officers responding to calls for service and in the course of investigations (RCMP, 2010).

[36] "The RCMP requires approval from the Minister of Public Safety to disclose a criminal file containing pardoned sexual offenses to a police service, and a police service requires written consent from the subject of the search to disclose the criminal file to the requesting organization, pursuant to the Criminal Records Act" (RCMP, 2014b).

[37] CFIS is a register of Canadian firearms license holders.

CAN 3. Addressing Canadian Police Information Centre Data Quality and Completeness

Criminal-history data held in the NRCR are subject to several limitations. This section discusses the completeness of NRCR data, their quality, ways to overcome these limitations, and ongoing efforts to monitor and make improvements in these areas.

CAN 3.1 Data Completeness

The lack of completeness of NRCR data is currently the biggest challenge in their use for operational and research purposes. Most significantly, there is a delay between a court action (e.g., conviction) and when the corresponding record is uploaded into the NRCR.[38] This has potential implications for operational uses. For instance, if a person moves from one jurisdiction to another, their criminal history may not be discoverable for some time.[39] The delay in updating the NRCR has also been noted as a challenge in the context of sentencing, where judges may be prevented from taking the entirety of a person's criminal record into consideration (Bureau, 2015).

The backlog in updating the NRCR has been a matter of concern for some years. For instance, a 2009 report by the Auditor General of Canada stressed the issue and noted it had deteriorated over the preceding five years (OAG, 2009). The volume of outstanding records continued to grow, reaching about 570,000 FPS files waiting to be uploaded onto NRCR as of August 2016.[40] Given that at that time the repository held approximately 4,458,000 files, the backlog amounted to approximately 11 percent of files supposed to be on the NRCR (RCMP, 2016c). Since 2016, the backlog has declined, and, according to information provided by the RCMP, it stood at approximately 380,000 files as of March 2018. The RCMP is working to eliminate the backlog.

Other issues surrounding data completeness stem from the NRCR's institutional arrangements. First, the scope of information to be captured on the NRCR is limited. The repository does not hold data on stand-alone summary offenses, although agencies may report this data if summary offenses are accompanied by hybrid or indictable ones. Similarly, nonconviction data may or may not be reported to the RCMP. Second, data that are reported to the NRCR can be removed under certain circumstances. As discussed in Section CAN 2.2, convicted individuals have the option to apply for a record suspension, after which, if their application is successful, the record of their conviction is not visible on the NRCR.

---

[38] Theoretically, the two possible sources of delay are (1) a local agency taking some time submitting information to the NRCR; and (2) the RCMP processing submitted information and uploading it onto the NRCR. The introduction of CJIM technology (discussed later in this section) addressed the second potential source of delay.

[39] That is because while local and/or provincial databases in the place of previous residence would continue to hold information on the person's convictions, these databases would not be consulted after a person moves out of their jurisdiction.

[40] See, for example, OAG (2011).

CAN 3.2 Data Quality

There are no publicly available official assessments of the quality of data held in the NRCR. In contrast with the issue of upload delays discussed above, no sources reviewed in the course of this study have raised data quality as an issue affecting the NRCR. Importantly, however, the responsibility for ensuring the accuracy of data does not rest with the RCMP but with the contributing agencies (OPC, 2011). In that regard, concerns have been raised about the quality of police data in Canada produced and held at the local level.[41] This is perhaps less applicable to information on criminal proceedings and court dispositions; however, issues with police data have been noted in such areas as inadequate/incomplete recording of information on offenses, substandard file descriptions and synopses, and coding of data.[42]

CAN 3.3 Efforts to Overcome Record System Deficiencies

The RCMP has initiated a number of efforts to address the backlog of criminal records in the NRCR. Between 2004 and 2013, the RCMP undertook the Real Time Identification project, which replaced paper-based processing of fingerprints with digital methods, leading to reductions in verification times (RCMP, 2013). Building on this project, since 2015, all fingerprint submissions to CCRTIS have been done electronically (Senate of Canada, 2016). Furthermore, in 2016, RCMP carried out a pilot project allowing law enforcement agencies to submit court disposition information electronically and thus shorten the time required to send updates to the NRCR (RCMP, 2016d). A full rollout of the initiative, the CJIM project, is currently underway (Senate of Canada, 2016).

In FY 2015/16 and FY 2016/17, the RCMP also increased its NRCR budget and the number of analysts responsible for the upload of information onto the NRCR to address the backlog (RCMP, 2016c). In addition, in an effort to manage caseload and risks associated with the backlog, the RCMP has divided data into several priority categories (Senate of Canada, 2016). An example of high-priority data is information on recent convictions of individuals under 25 years of age. The RCMP has also provided agencies with the option of requesting an expedited upload of particular records, for instance, in connection with parole board hearings and/or sentencing decisions (Senate of Canada, 2016).

With respect to the content of the records, as mentioned above, the responsibility for CPIC data accuracy rests with the contributing agencies (OPC, 2011). Historically, the RCMP would send individual agencies regular validation reports containing all CPIC entries provided by the agency that have been on the system for at least 12 months (OPC, 2017). This report would invite agencies to verify the accuracy of entries they provided to CPIC and make any amendments necessary. In addition, each participating agency would be audited onsite at least

[41] See CAN-SEBP (n.d.).

[42] See McCormick et al. (2007) and Huey (2017).

once every four years to assess its compliance with the validation process, along with other policies, such as privacy and data security arrangements (OPC, 2011). Following the completion of a pilot project in 2015, the RCMP is currently in the process of implementing a new approach to ensuring data integrity, quality assurance review (QAR). The new process represents a departure from the old audit cycle and introduces a risk-based approach to quality control. Under the new system, all police chiefs in Canada will receive a QAR report, the first edition of which will set up national baselines in an effort to capture trends in system and data integrity. The QAR aims to help agencies develop or strengthen their strategies to mitigate data integrity risks (RCMP, 2016b). As of June 2016, approximately half of CPIC law enforcement records had undergone a review under the new audit system, and QAR reports had been sent to the respective originating agencies (RCMP, 2016d).

Several additional arrangements help contributing agencies with ensuring the quality of data. The procedures for data management and data use on the NRCR are standardized (Kilgour, 2013). As discussed in Section CAN 2.1, a standardized RCMP form is used to create a fingerprint record by the local agency and for an eventual upload onto the NRCR. For users with update and/or maintain privileges to the Investigative or Intelligence Data Banks, the RCMP runs a maintenance course (RCMP, 2016a). Numerous contributing agencies have dedicated CPIC-related posts among their staff, such as CPIC validators, responsible for the verification and validation of information provided by the agency to CPIC and for liaison with the RCMP.[43]

More broadly, two additional factors support criminal justice data quality in Canada. First, the fact that Canada has one criminal code applicable to all provinces and territories not only helps to ensure consistency in the administration of criminal justice across the country but also helps mitigate such issues as differences in definitions or lack of offense and sentence equivalence across jurisdictions. Second, there is currently a strong degree of standardization with respect to local police records due to the fact that the vast majority of law enforcement agencies (at all levels of government) utilize one of two types of record management software. This means that in practice police data are recorded and stored in a very limited number of ways. In addition, if the type of data collected by local agencies needs to be modified (e.g., if Statistics Canada and its Canadian Centre for Justice Statistics are interested in capturing a new variable or in modifying an existing one), discussions and coordination need to involve a small number of software providers.

[43] See Windsor Police Service (n.d.).

CAN 4. How Are National Repository of Criminal Records Criminal-History Record Data Used for Research Purposes?

CAN 4.1 Access to National Repository of Criminal Records Data for Research Purposes

According to the "Ministerial Directive Concerning the Release of Criminal Record Information by the Royal Canadian Mounted Police," NRCR data can be accessed for research purposes by "research groups conducting studies which are related to the execution or administration of the law, including evaluation of treatment or correctional programs, when the research is being conducted by or on behalf of a Canadian police service, a provincial, territorial or federal Attorney General of Solicitor General or minister responsible for Justice, corrections or policing."[44]

According to an interviewee with experience in conducting research with NRCR data, to gain access, a researcher needs to file an application with the RCMP detailing the objectives of the research, the intended use of the data, and the proposed data retention period. Once the application is approved and fees paid based on the number of records requested, the RCMP provides a nonanonymized data set to the researcher. The nonanonymized data are subject to a retention period agreed on in the research application, but recoded data (with recoding done by researchers) can be held indefinitely.

One interviewed academic researcher was able to offer his perspective on accessing NRCR data through collaboration with a local RCMP agency. Generally, according to the academic interviewee, when approaching the RCMP, external applicants need to outline a very specific use of data in their request, specifying which individuals will be included, why, what type of information is needed, and how the data will serve the project goals. Often, the process will require a formal partnership with a law enforcement agency. The RCMP will review the proposal in an internal committee and assess its utility and alignment with the RCMP's priorities. While there is no formal ethical board at the RCMP, they will ask for an ethics approval certificate from the applicant's home institution (e.g., a university) and will include it in the proposal consideration. After the application is granted and data retrieval is completed, all names and birth dates are purged and replaced with a numeric ID and "age at X date." This is done to analyze the data outside an RCMP facility, with other precautions on data handling and security added for storage and password-protected data access. Another interviewee added that the ability to access RCMP data may depend on researchers' professional networks and existing working relationships with the agency. These not only help facilitate any requests for data but also may lead to instances when a researcher is approached by the RCMP to undertake a research project.

[44] The document is not publicly available. Information was provided by the RCMP.

CAN 4.2 Possibilities and Limitations of the Use of National Repository of Criminal Records Data for Research Purposes

NRCR data have been used to analyze criminal trajectories through formal interactions with the criminal justice system.[45] Researchers have used NRCR data to analyze the length and other attributes of criminal careers (from first conviction to most recent).[46] NRCR data can also be used to analyze the range of crimes offenders are involved in, exploring such issues as whether they commit predominantly violent offenses or whether they commit a variety of crimes.[47]

The limitations of the NRCR as a resource for research are related to issues discussed in Chapter 3. These include the delay in uploading criminal-history information onto the NRCR and its limited scope, as summary offense and nonconviction information may or may not be reported.[48] Furthermore, several interviewees confirmed it is not possible for researchers to know what record suspensions have been granted and, therefore, what conviction records may not be visible in the data set.[49]

Overall, however, numerous academic interviewees noted that relatively little research is undertaken with NRCR data, and it is relatively difficult for researchers to obtain access to these data. One interviewee opined that there were substantial administrative requirements associated with applying for CPIC access, prompting many researchers to pursue other data sources. In addition, in the limited number of instances CPIC data have been used, it is possible to negotiate access to the database through a local CPIC agency, obviating the need to go through formal arrangements with the RCMP. Interviewees who commented on the topic agreed that the best option available to researchers is to enter into a partnership with a local or provincial agency that is able to provide access to CPIC data. In this context, subnational agencies are also an option to researchers because they generate and report the data that are held in CPIC. These agencies, therefore, hold the same data as CPIC, in addition to data that were not reported to CPIC, although they are naturally limited in terms of geographical scope. Research collaborations with local and provincial agencies are governed by their own policies and procedures, which vary across individual jurisdictions. There is no national standard for research collaborations involving local agencies, and arrangements put in place by local agencies may vary.

---

[45] See Wheeler, Worden, and McLean (2016).

[46] See Mathesius and Lussier (2014).

[47] See Hilton and Eke (2016).

[48] An interviewee offered an example of evidence of this delay in practice. In one project combining NRCR and corrections data, an individual was listed in the corrections database as having been booked into a correctional facility. However, there was no record of the corresponding conviction on the NRCR.

[49] While this arguably represents a less important uncertainty, data on nonconvictions may also be removed depending on whether individuals have applied for their deletion and their applications have been granted. The lack of clarity on nonconviction data is compounded by (1) the lack of standards or common approaches on when nonconviction data are reported to CPIC in the first place and (2) uncertainties surrounding the extent to which local agencies forward their deletion decisions to the RCMP.

4. England and Wales

Key Findings

- Established in 1974, the Police National Computer (PNC) is the primary national-level criminal-history information system used in England and Wales.
- PNC data are submitted and accessible by all police forces and law enforcement agencies throughout England, Wales, Scotland, and Northern Ireland.
- The PNC captures information on arrests, cautions, reprimands, warnings, and convictions, as well as noncriminal-history information, such as banning orders, driving disqualifications, and registration as a firearm owner.
- Each individual with a criminal record is assigned a unique PNCID for the rest of his or her life that is used in any interaction with the criminal justice system. The PNCID will never be reissued and is the most common identifier used in searches of the PNC.
- Criminal records are retained on the PNC until the individual's 100th birthday.
- The chief officer for each police agency where the PNC record originated retains ownership over the data contained in that record. Agencies may exercise their discretion to delete noncourt disposals (such as cautions) and nonconviction outcomes from their records, although in practice this rarely occurs.
- Fingerprints (and DNA where available) are used to link an individual's criminal-history record information and help to ensure the accuracy of the data.
- The PNC is used by law enforcement agencies across the UK to share information and facilitate criminal investigations. Police are also responsible for updating PNC records with court data, although almost all courts can connect to a portal that automatically transmits outcomes to the PNC.
- In addition, approximately 60 organizations have read-only access to information on the PNC to help them fulfill their statutory functions. They will either link their systems to it or obtain information from a read-only access portal.
- PNC data are used to perform background checks on individuals (e.g., during preemployment checks), and individuals may apply for access to see the information held on them in the PNC.
- Non-law-enforcement organizations (not including researchers) may apply for access to criminal-history information held on the PNC through the PNC Information Access Panel (PIAP).
- Researchers may apply for access to an extract of the PNC housed by the Ministry of Justice (MOJ) through the MOJ's Information Access Panel (MIAP).
- Due to its age, the PNC uses relatively old information technology that prevents modern use of the data, such as advanced analytical processes, and limits how much data can be shared.

E&W 1. Overview of the Countries and Criminal Justice System

E&W 1.1 Political and Constitutional System

The United Kingdom of Great Britain and Northern Ireland is a constitutional monarchy, with a population of about 66 million (ONS, 2018). The UK is both a constitutional monarchy and a participatory democracy, which means that the government and Parliament make political decisions rather than the reigning monarch. The UK is composed of four countries—England, Wales, Scotland, and Northern Ireland. There is no written constitution, although the term *constitutional law* is often used to refer to such matters as the role of the state and the protection of rights (King, 2001). Furthermore, statutes passed by Parliament are not subject to review by the courts. As a result of a long process of devolution, the UK government is responsible for criminal justice matters only in England and Wales. Scotland and Northern Ireland each has its own, separate criminal justice system, although there are commonalities and links between the systems.

E&W 1.2 Criminal Code and Procedure

England and Wales do not have a criminal code, and many criminal offenses have no basis in legislation but rather are a matter of common law, developed by the courts. The age of criminal responsibility in England and Wales is ten years old.

There are three types of offenses heard in courts in England and Wales. Summary offenses are less serious offenses, such as minor assaults or driving offenses. These kinds of offenses are typically disposed of in magistrates courts, where defendants are not entitled to a jury trial. "Either way" offenses can be heard either by a magistrate or by a judge and jury at the Crown Court. These are generally more serious offenses, such as theft or handling stolen goods. For these cases to go to the Crown Court, a defendant can insist on a jury trial, or a magistrate can decide that the matter is serious enough for the Crown Court. Finally, offenses may be indictable only, which means they can be heard only by the Crown Court. These offenses are the most serious and include murder, manslaughter, and rape. Before such a case goes to the Crown Court, the magistrates court typically makes a decision on granting bail to the defendant.

E&W 1.3 Court Dispositions and Penal Sanctions

There are several ways in which criminal charges can be resolved in court in England and Wales. Most defendants (87 percent in 2018) plead or are found guilty, a ratio that has held steady in recent years (MOJ, 2019). The most common type of sentence imposed is a fine, particularly for summary offenses: 77 percent of sentences were fines in 2018, with the vast majority of fines (96 percent) imposed for a summary offense. A custodial sentence, or imprisonment, is imposed when the offense committed is "so serious that neither a fine alone nor

a community sentence can be justified for the offense."[50] When the period of custody imposed by the court is between 14 days and 2 years in the Crown Court or 6 months in the magistrates court, an offender may also receive a suspended sentence. The sentence may be suspended for up to 2 years, during which time the offender must not reoffend, must avoid problems with the law, and may have to follow certain conditions of their release, such as a curfew or participation in a drug- or alcohol-treatment program. If these terms are not complied with, the offender is typically ordered by the court to serve both the original sentence and any additional penalty for the latter offense(s) (Sentencing Council, n.d.c). A community order imposes requirements on an offender, to be completed with the probation service over a set period (the sentence length). Requirements can be a set number of hours of unpaid work, curfew, or participation in an alcohol- or drug-treatment program. An offender may be given a discharge for matters involving the least serious offenses, such as minor theft. This may be an absolute discharge, where no formal punishment is imposed but the offender receives a criminal record, or a conditional discharge, which means that if the offender commits another crime, they can be sentenced for both offenses at the second trial (Sentencing Council, n.d.a). Finally, in a small number of cases, a court may order the offender to pay compensation for their offense (Sentencing Council, n.d.b).

E&W 1.4 Criminal Justice Agencies

Law enforcement: There are 43 regional (or territorial) police forces across England and Wales, each of which has jurisdiction over a specific geographical area. Together, they assume the majority of policing responsibilities. In addition, there are a small number of national law enforcement agencies, which are referred to in the Serious and Organised Crime and Police Act 2005 as "special police forces." These include the National Crime Agency (NCA), which targets serious and organized crime, and the British Transport Police (BTP), which polices the UK's railways and several public transport networks. The NCA works across England and Wales, and in Scotland and Northern Ireland with the permission of the relevant domestic prosecuting office. The BTP operates across England, Wales, and Scotland.

In addition, there are many miscellaneous police forces that typically have policing responsibilities for a specific local area or activity, such as a port. Officers from the 43 regional police forces and the BTP have certain powers of arrest in all jurisdictions of the UK. Furthermore, Her Majesty's Inspectorate of the Constabulary and Fire and Rescue Services (HMICFRS), which until 2017 was known as Her Majesty's Inspectorate of Constabulary (HMIC), has responsibility for the inspection of police forces in England and Wales, including the NCA and the BTP.

Prosecutors: The principal prosecuting authority for criminal cases in England and Wales is the Crown Prosecution Service (CPS), which was established in 1986. The CPS works with the police and other investigators advising on lines of inquiry and deciding whether to pursue

[50] Section 152(2) of the Criminal Justice Act 2003.

particular charges or other outcomes (Crown Prosecution Service, n.d.). A chief Crown prosecutor leads each of the 14 geographical areas of operation across England and Wales. The CPS may present cases in both the Crown Court and the magistrates courts, described below.

Courts: Almost all criminal cases start in the magistrates courts. These cases are typically heard by a panel of two or three magistrates; as of 2019, there are approximately 16,000 magistrates working in 330 courts in England and Wales (Courts and Tribunals Judiciary, n.d.). Magistrates are justices of the peace and work on a voluntary, unpaid basis. No legal qualifications are required for this role, but magistrates are given legal and procedural advice by justice's clerks. There is also a much smaller number (140) of district judges, who are typically based in larger cities. District judges are full-time, paid professionals with legal qualifications. Most cases heard in the magistrates courts are brought by the CPS, but several other agencies, such as the Department of Work and Pensions and the Environment Agency, also have the power to prosecute cases. Where a defendant offers a guilty plea or is found guilty by the magistrates, they proceed to sentence following a structured decisionmaking process, as well as official sentencing guidelines (Courts and Tribunals Judiciary, n.d.). In youth courts, different sentences are available to better serve the needs of youth offenders. As of 2019, the vast majority (over 95 percent) of criminal cases are heard in the magistrates courts (Courts and Tribunals Judiciary, n.d.).

The Crown Court typically deals with more serious offenses, appeals of decisions made in magistrates courts, and defendants convicted in the magistrates courts but, due to the seriousness of their offense(s), who have been sent to the Crown Court for sentencing. Cases are heard by a judge and a jury, but it is the jury who decides the guilt or innocence of the defendant, usually by a unanimous but also occasionally a majority decision (Judicial Office International Team, 2016).

Corrections: Her Majesty's Prison and Probation Service (HMPPS) has responsibility for prison and probation services across England and Wales. Within HMPPS are two different units: Her Majesty's Prison Service, which manages 109 public prisons and manages the contracts for an additional 14 private sector prisons (HM Prison Service, n.d.), and the National Probation Service, which is responsible for preparing presentence reports for courts, managing approved premises for offenders where required, assessing offenders in prison prior to a conditional release, assisting offenders who are serving sentences in the community to meet their court-ordered requirements, and liaising with victims of serious sexual and violent offenses.

E&W 1.5 Size of Criminal Justice System

According to police recorded crime data, which is supplied to the Office for National Statistics (ONS) by the Home Office, in 2018, there were over 5 million offenses recorded by police forces in England and Wales, corresponding to a rate of 88 per 1,000 population (ONS, 2019). According to the MOJ, about 1.6 million individuals, including both people and companies, were processed through the criminal justice system in England and Wales in 2018. Of these, approximately 1.4 million defendants were prosecuted at court in 2016 (MOJ, 2019). In June

2018, approximately 83,000 people were imprisoned in England and Wales, corresponding to an incarceration rate of slightly above 140 inmates per 100,000 population (HM Government, 2019).

E&W 2. Understanding the National Criminal-History Record System

E&W 2.1 History and Organizational Management

The primary national-level criminal-history information system used in England and Wales is the PNC, which is governed by Section 27(4) of the Police and Criminal Evidence Act 1984.[51] It is accessible by all police forces and law enforcement agencies throughout England, Wales, Scotland, Northern Ireland, the Isle of Man, and the Channel Islands, including the BTP.[52] The PNC was started in 1974, initially as a database of stolen vehicles. It has been expanded with new information and applications in almost every year since then and now contains several separate databases holding and linking information on criminal history, as well as vehicles, motorists, and missing or found property, and has direct links to several other external databases. Criminal-history information held in the PNC is mainly inputted by designated users within individual police forces, who are all responsible for updating the database with their own records. The BTP does not update the PNC as the force does not have its own custody suite; therefore, most of the BTP's arrests are made by officers from other forces, who update the PNC on their behalf. Most courts update the PNC with the outcome of cases through a portal to the system, using the arrest summons number, while a small number of courts send case updates to police forces manually.

E&W 2.2 Content

A nominal record (i.e., a record pertaining to a specific individual) may be created for a number of reasons. As evidenced in Table 4.1, not all nominal records in the PNC relate to criminal history.

[51] Unless indicated otherwise, this and the subsequent sections of the England and Wales chapter primarily draw on expert input and interviews with key informants familiar with or involved in the management of the PNC. According to Section 27(4) of the Police and Crime Evidence Act 1984, "The Secretary of State may by regulations make provision for recording in national police records convictions for such offences as are specified in the regulations." In subsection (4A) "conviction" is defined as including "(a) a caution within the meaning of Part 5 of the Police Act 1997; and (b) a reprimand or warning given under Section 65 of the Crime and Disorder Act 1998" (Legislation.gov.uk, n.d.).

[52] Scotland and Northern Ireland each has its own database, which interfaces with the PNC.

Table 4.1. Reason for Police National Computer Record Creation

Reason for PNC Record Creation
• A person has been arrested, charged, or reported for summons for the commission of or involvement in a recordable offense (generally defined as an offense that could result in imprisonment).[53]
• A person is wanted for committing a specific offense.
• A person is wanted for the nonpayment of fines imposed by a court.
• A person has failed to appear at a court in answer to a charge made against them.
• A person has been excluded from entering certain establishments (e.g., football grounds, licensed premises, etc.) by a court.
• A person has been reported missing or has been found.
• A person has absconded from or is subject to recall to a detention center, prison, youth custody, remand center, and so on.
• A person has deserted from the armed forces.
• A person's whereabouts are sought for other police purposes (e.g., as a witness to an incident).
• A person has been disqualified from driving a motor vehicle on a road by a court.
• A person is the subject of a particular type of court order.
• A person has an entry on the National Firearms Licensing Management system.
• A person is the subject of a record originally created and held at the National Identification Service (a support service within London's Metropolitan Police).

As of October 2014, there were approximately 11.5 million nominal records (pertaining to specific individuals) on the PNC, of which about 10.5 million contained a criminal record element, including convictions, cautions, reprimands, warnings, and arrests[54] (Beard, 2019; Home Office, 2015).

[53] Where an offense exists only in a certain jurisdiction, such as Scotland or Northern Ireland, the offense will be identified as such in the PNC. Similar offenses across jurisdictions are grouped together in the PNC, so a search of the PNC for a particular offense will return results for all like offenses.

[54] In Scotland, unlike other UK jurisdictions, three verdicts are available at a criminal trial: "guilty" (a conviction), "not proven," and "not guilty" (both types of acquittals). The PNC can record these types of verdicts, along with the guilty and not-guilty verdicts used in other jurisdictions.

Cautions are formal warnings that may be given by the police to persons aged 18 or over who admit to committing an offense. Cautions are given in cases of low-level, mainly first-time offending without a prosecution. A conditional caution is a caution with conditions for the offender attached, such as entering a drug-treatment program. Youth cautions are a formal out-of-court disposal that can be used for offenders aged 10 to 17 years old, where the offender admits the offense but it is not in the public interest to prosecute.

Each record is allocated any one or a combination of the following categories: offense processing (criminal record), wanted or missing, disqualified driver, or firearms certificate. The record will contain some nominal data, including such search factors as name, date of birth, sex, skin color, height, and any other identifying details, as well as noting the sources of information and warning of any potentially dangerous behaviors. It will also contain identification numbers, such as a system-generated PNCID if the person has been charged with an offense, a Driver Vehicle Licensing Agency (DVLA) driver number, and a Criminal Records Office (CRO) number, if applicable. The PNCID is a unique number assigned to the criminal-history record, completely independent from the CRO number, which is assigned to the individual for the rest of his or her life and used in any interaction with the criminal justice system. It will never be reissued and is the most commonly used identifier in searches of the PNC. A CRO number is generated by the National Fingerprint Database IDENTl, when an individual is identified using fingerprints, and similarly, only one CRO number is issued per person regardless of aliases they may use. Record searches may use either a combination of name, date of birth, sex, color, and height or a PNCID or CRO number.

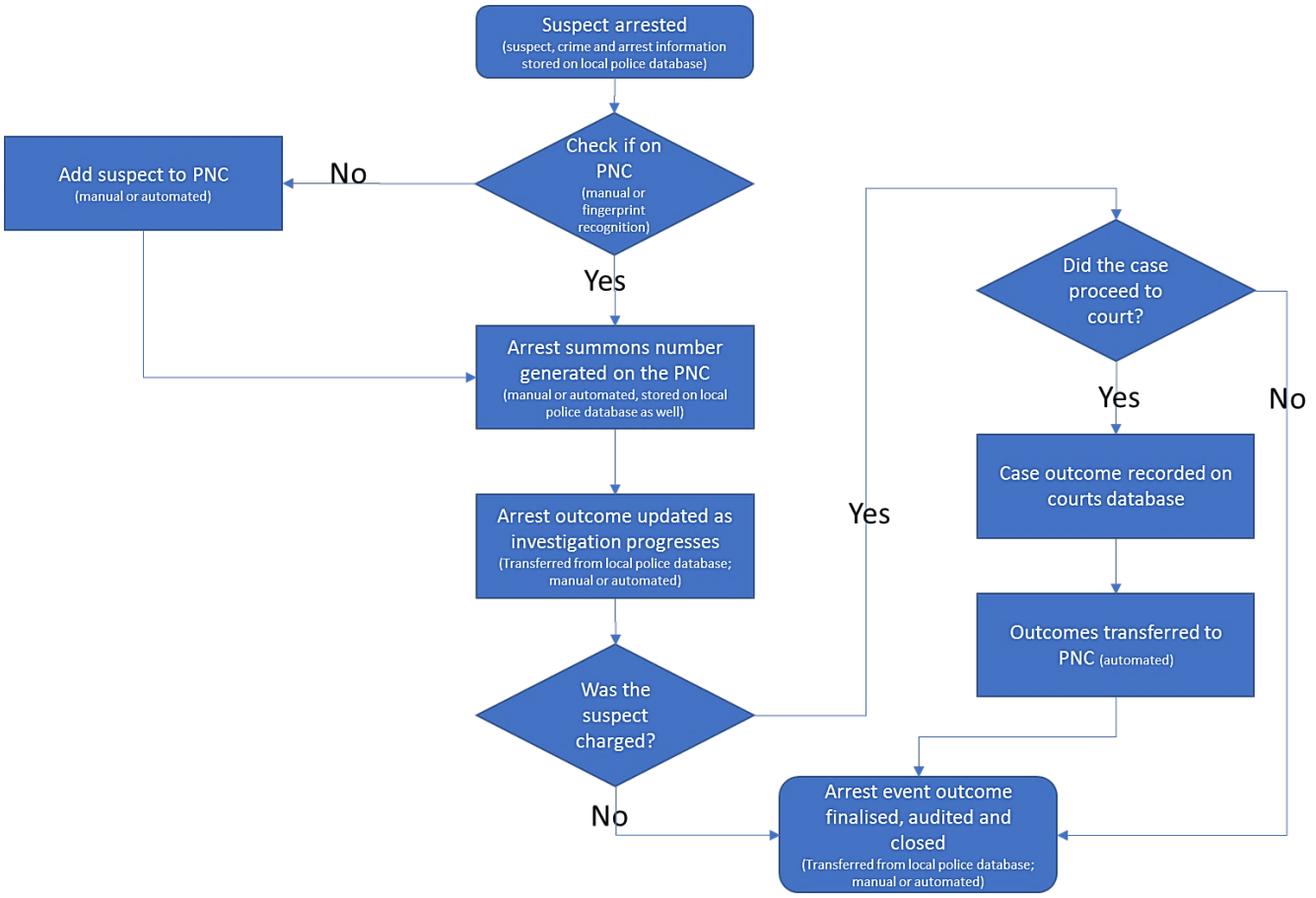
Creating a Police National Computer Record

PNC records can be created by any police force operating in any jurisdiction within the UK or by any law enforcement agency with relevant permissions to do so, when exercising their lawful duties within the UK or abroad (NPCC, 2018). More detail on these organizations is included in Section E&W 2.4 of this chapter. Almost all PNC records are created and updated by the police (for more information, see Section E&W 3.1). Figure 4.1 describes the process to update the PNC from arrest to, if applicable, court outcome.

A reprimand was a formal verbal warning given by a police officer to a young person who admitted a minor first offense. They were replaced by youth cautions in 2003.

Final warnings were also replaced by youth cautions in 2003. Other warnings, such as harassment warnings or cannabis warnings, are not included in PNC records.

Figure 4.1. Process to Update the Police National Computer



Within each police force is a PNC bureau team that is responsible for ensuring the police force is compliant with the PNC procedures. The exact processes used to enter data into the PNC vary by police force due to local information technology systems, local historical practices in managing criminal-history data, and available resources. A general process is described below with reference made to potential differences between police forces.

Arrest of a Suspect

The new arrestee's information is recorded into the police force's custody management system when they present at the police station (specifically when they are booked into a custody suite).[55] In some forces, fingerprints are checked electronically in the custody suite, and, through links to IDENT1, whether the individual is already on the PNC is flagged from their fingerprint record. The local arrest record created must then be manually added to the PNC (time of arrest, outcome, etc.). The PNC bureau will check if an individual is already on the PNC and record the

[55] A custody suite is an area inside a station where people who have been apprehended by the police are held prior to being remanded by the courts or released.

individual's PNCID number on the local system if it is missing or if the suspect has not previously offended. Newer police systems, however, have automated the record creation and editing process, as well as the retrieval of information from the PNC. (Due to the technological limitations of the PNC, this can involve screen scrapes.) If an individual provides a false name and it is entered into the PNC, their record will always be held under that name, with the individual's real name listed as an alias and linked by fingerprint records. The reason for this approach is to create an audit trail for the person's record. Under the PNC code of practice, an arrest or summons must be entered into the PNC within 24 hours.

Following the Arrest Event to Disposition

An arrest can have four basic outcomes: no further action or an out-of-court disposal, both of which are recorded by police; a court conviction; or a court acquittal, for which the court provides PNC updates. An arrest summons number is created on the PNC for an arrest, and that number follows the suspect through the incident and on to court for confirmation of conviction. Further police updates—such as the outcome type or the crime type—are either entered by the PNC bureau team within the police force or are automated and checked by the PNC team. The courts in England and Wales have two computer systems—Libra for the magistrates court and the Crown Court case management system—and each can update the outcome of a case in the PNC using the arrest summons number. Court data are typically updated automatically through a portal to the PNC, but a small number of courts send updates to police forces manually. Under the PNC code of practice, the police are responsible for ensuring that PNC records are updated with court data within ten days of the information being submitted to them.

E&W 2.3 Data Retention

Before 2006, criminal-history records in England and Wales could be deleted by the police after a certain period, depending on the criminal history of the individual.[56] Where an individual had not been convicted of a recordable offense (an offense that could result in imprisonment) for 10 years following the date of their last conviction, the record would be deleted. However, if the individual's record contained three or more convictions for recordable offenses, the record would be retained for 20 years from the last conviction. Moreover, a conviction record would be retained until the individual's death or 100th birthday where

- the record contained prison sentences totaling six months or more, including suspended sentences

[56] Scotland has its own data retention rules, which is managed through its local system. When a record in the Scottish system is deleted, the interface is automatically triggered, and that record is deleted in the PNC. The most common differences in retention rules between Scotland and England and Wales relate to low-level offenses. As the Northern Ireland system is in its infancy, it currently follows the data retention rules of England and Wales, although this may change.

- the offender had at any time been found unfit to plead by reason of insanity or had been sentenced under the Mental Health Acts
- the offender had convictions for offenses involving indecency, sexual offenses, violence, or class A drugs, such as heroin or cocaine
- the offender deliberately targeted a child or young person, an elderly person, or someone who is mentally or physically disabled.

Records containing cautions but not convictions would be deleted if no further cautions were recorded for five years, except where the individual offended against a vulnerable person. Where a record contained police reprimands or final warnings but no convictions, it would be deleted after the offender turned 18 years old and for a minimum period of five years from the date of the reprimand or final warning, provided there had been no further such disposals during that time.

In 2006, a new policy was introduced whereby all records are retained on the PNC until the individual's 100th birthday. In certain circumstances, an individual may still apply to a police force to have a record of noncourt disposals (e.g., cautions or nonconviction outcomes) deleted in the PNC, as well as the National DNA Database (NDNAD) and IDENT1. As each force's chief officer "owns" the data that their force has entered onto the PNC, they may exercise discretion to delete records that have been entered by their force (Beard, 2019). To ensure a consistent approach to the exercise of this discretion, the National Police Chiefs' Council (NPCC) has issued guidance on the deletion of records from national police systems (NPCC, 2018). This guidance does not set specific criteria for record deletion but rather provides examples of circumstances in which consideration of the application may be given by the chief officer. Individuals with a court conviction or who are subject to an ongoing investigation or court proceedings cannot apply to have their records deleted. Circumstances that may be considered in an application for record deletion are set out in the guidance and presented in Table 4.2. However, according to consulted experts, instances in which a request to delete a record was approved are rare.

Table 4.2. Grounds for Police National Computer Record Deletion

	Grounds for PNC Record Deletion
No crime	Where it is established that a recordable crime has not been committed. For example, a sudden death where an individual is arrested at the scene and subsequently charged, but after post mortem it is determined that the deceased person died of natural causes and not as a result of homicide.
Malicious/false allegation	Where the case against an individual has been withdrawn at any stage and there is corroborative evidence that the case was based on a malicious or false allegation.
Proven alibi	Where there is corroborative evidence that the individual has a proven alibi and as a result s/he is eliminated from the enquiry after being arrested.
Suspect status not clear at the time of	Where an individual is arrested at the outset of an enquiry, the distinction between the offender, victim and witness is not clear, and the individual is subsequently eliminated as a

arrest	suspect (but may be a witness or victim).
Incorrect disposal	Where disposal options are found to have been administered incorrectly and under the correct disposal there would be no power to retain the DNA profile. In such circumstances, consideration should be given to deleting the DNA profile, fingerprints, and the PNC record. Deletion in these circumstances could also be the product of review within the criminal justice process, for example, the withdrawal of a caution.
Judicial recommendation	If, during court proceedings, a magistrate or judge recommends that an individual's DNA and fingerprints should be deleted. On such occasions, due consideration should be made in relation to the deletion of the PNC record.
Another person convicted of the offense	If there is a conviction of another person for the offense, then the Chief Officer may wish to consider the deletion of the biometric information and PNC record, provided there in no possibility of there being more than one offender.
Public interest	Where there is a wider public interest to delete the PNC record.

SOURCE: NPCC (2018).

Retention of Biometric Information

Under the Police and Criminal Evidence Act 1984, the police may take a DNA sample of a person who has been arrested for, charged with, or convicted of a recordable offense or who has consented to having their DNA taken. This sample is converted into a DNA profile and stored on the NDNAD. A marker is added to the PNC to highlight that a record is held on the NDNAD for the individual. Since the PNC does not have the capability to store images, a person's PNC record contains a link to their record on the NDNAD, where such a record exists.

The rules for gathering and retaining fingerprints in IDENT1 are the same as for DNA profiles. As with any NDNAD record, a person's record on IDENT1 would be linked to from their PNC record, where such a record exists. Following the Protection of Freedoms Act 2012, a new governance regime for the retention of DNA information and fingerprints was introduced in England and Wales. Under this act, there is a general presumption that biometric information will be destroyed where an individual was not convicted of any offense. If a DNA profile should no longer be stored on the NDNAD, the PNC will create an alert for the police force that created the relevant records, and a system administrator will delete the appropriate data.

The act sets out the retention periods for biometric information, which are listed in Tables 4.3 and 4.4.

Table 4.3. Biometric Retention Periods: Individuals Convicted of an Offense

Situation	Fingerprint and DNA Retention Period
Adult convicted (including cautions, reprimands, and final warnings) of any recordable offense (generally defined as an offense that could result in imprisonment).	Indefinite.
Person under age 18 convicted (including cautions, reprimands, and final warnings) of a qualifying offense (defined in Section 65A of the Police and Criminal Evidence Act 1984 as more serious offenses such as murder, kidnapping, and sexual offenses).	Indefinite.
Person under age 18 convicted of a minor offense (defined as any recordable offense that is not a covered under the definition of a qualifying offense).	First conviction: 5 years (plus length of any custodial sentence), or indefinite if the custodial sentence is 5 years or more. Second conviction: Indefinite.

SOURCE: ACRO (n.d.).

Table 4.4. Biometric Retention Periods: Individuals Not Convicted of an Offense

Situation	Fingerprint and DNA Retention Period
Any age charged with but not convicted of a qualifying offense	3 years and a 2-year extension if granted by a district judge (or indefinite if previously convicted of a recordable offense that is not excluded from retention rules—see Table 4.2).
Any age arrested for but not charged with a qualifying offense	3 years if granted by a biometrics commissioner and a 2-year extension if granted by a district judge (or indefinite if previously convicted or a recordable offense that is not excluded from retention rules).
Any age arrested for or charged with a minor offense	None (or indefinite if there is a previous conviction for a recordable offense that is not excluded from retention rules) but speculatively searched against the NDNAD and IDENT1.
Penalty notice for disorder	2 years.

SOURCE: ACRO (n.d.).

In certain circumstances, an individual may apply to a chief officer of the police force that created the relevant record to have their biometric information deleted before the end of the retention period. An example of qualifying circumstances would be if the individual had no previous convictions and their biometric information was being held due to a penalty notice for disorder.[57] The NPCC's guidance to chief officers provides advice on the retention of biometric information (NPCC, 2018).

[57] A penalty notice for disorder is a fine for low-level, antisocial, and nuisance offending.

Pardons

The monarch may exercise the POM to pardon an individual convicted of an offense, on the recommendation of the secretary of state for justice. There are two types of pardons. A free pardon, which has typically been granted in cases of miscarriages of justice, relieves the convicted person of any punishment imposed or other consequences of their conviction. A conditional pardon may be granted to mitigate the penalty imposed originally and was historically used to commute death sentences to life imprisonment. Information about these matters will remain in the PNC but will not be disclosable in certain circumstances.

E&W 2.4 Access to the Police National Computer for Operational and Civil Purposes

Institutional Access for Operational Purposes

In addition to being used by law enforcement agencies across the UK to share information and facilitate criminal investigations, the PNC is read-only accessible to approximately 60 organizations (many of which are agencies within the Home Office) to help them fulfill their statutory functions and will either link their systems to it or derive information from a read-only access portal. The PIAP, a centralized group composed of a cross-section of representatives from different forces, considers requests for access to the PNC. Requesting agencies are subject to vetting according to the level of access they require, which includes a security check of the physical environment and relevant information systems. Any organization given access will be asked to sign a code of connection and a supply agreement, which sets out the purpose of the application, the people who will have access to the data, requirements around the security environment, and other terms of access. Access is usually granted on a permanent basis, although some arrangements can be temporary.

Often agencies can request data for a specific individual but cannot themselves make any additions or edits to the records, although nonpolice prosecuting agencies may request that the ACRO Criminal Records Office create a PNC record for a defendant.[58] Being granted access to the PNC means the organization will be audited to ensure the data are used and stored correctly. HMICFRS conducts a regular program of inspections of nonpolice organizations with access to PNC data.[59] Nonpolice organizations are also subject to a separate Home Office audit, which examines whether the PNC data are held and used in an approved and secure way.

The following organizations have access to the PNC for operational purposes:

- **ACRO Criminal Records Office.** Responsible for managing criminal records in the UK and as such has full access to the PNC system. Based at the Hampshire Constabulary, it updates records on the PNC and supports prosecuting agencies to access PNC information, including making inquiry checks on their behalf. It also creates PNC records on behalf of

[58] ACRO stands for the Association of Chief Police Officers (ACPO) Criminal Records Office. ACPO was replaced in 2015 by the NPCC, but ACRO retains the abbreviation in its own name.

[59] Inspection reports are available from the HMICFRS website (Criminal Justice Inspectorates, n.d.).

nonpolice prosecuting agencies (see below) and converts historical criminal records held on microfiche to electronic records in the PNC. Any individual can ask the office what information is held about them on the PNC. ACRO also issues police certificates to people who want to immigrate to another country or obtain a visa. Lastly, ACRO's International Criminal Conviction Exchange shares criminal-history information with authorities abroad. This work is split between two teams: the UK Central Authority for the Exchange of Criminal Records, which exchanges criminal records between the UK and the central authorities of EU member states, and, the Non-European Union Exchange of Criminal Records team, which exchanges criminal records between the UK and non-EU Interpol countries via Interpol.

- **UK Visas and Immigration (Home Office agency).** Has access to the PNC to check the offending history of visa and residency applicants. When an individual applies for a visa, his or her fingerprints are checked against the fingerprint and immigration databases. If this provides a match to the criminal collection, the conviction record within the PNC is checked.
- **Nonpolice Prosecuting Agencies.** Organizations such as the Royal Society for the Prevention of Cruelty to Animals, the Environment Agency, the Post Office, Children and Family Court Advisory and Support Service, Gangmasters Licensing Authority, and the Financial Conduct Authority have the authority to prosecute members of the public. When doing so, the nonpolice prosecuting agency requests that ACRO create a PNC record. This generates an arrest summons number that is shared with the nonpolice prosecuting agency to administer the court process. If a conviction is reached, the courts systems update the result. Like other prosecuting bodies, nonpolice prosecuting agencies may request the disclosure of records when a prosecution is brought. Their access does not include firearms licensing, vehicle registrations, or any information that the nonpolice prosecuting agencies do not need to prosecute a case at court.
- **DVLA.** Responsible for registering all cars and all learner and qualified drivers. Stolen cars are registered on the PNC, and the PNC system informs the agency when a car is stolen. This prevents the agency registering the stolen car to a new user. Some individuals within the DVLA have access to the PNC for investigations. The agency system adds information to the PNC daily on vehicles involved in crimes.
- **HMPPS.**[60] Has read-only access to the PNC in order to complete assessments of offenders. Offender history is used to determine an individual's likelihood of reoffending.

Like Germany and the Netherlands, England and Wales exchange conviction information with EU member states via the UK Central Authority for the Exchange of Criminal Records. Information is also exchanged with non-EU Interpol countries through Interpol channels.

Access to Police National Computer Data for Civilian Purposes

Disclosure and Barring Service Check

Prospective employers may request a check of an applicant's criminal records through the Disclosure and Barring Service (DBS). Potential jurors at the Crown Court also undergo a

[60] Called the National Offender Management Service until April 2017.

DBS check. When the DBS has processed and completed a check, the applicant will receive a DBS certificate (DBS check). There are four types of DBS checks:

- **Standard check.** A standard-level certificate contains details of all convictions, cautions, reprimands, and final warnings held in the PNC that are disclosable in accordance with legislation (see the discussion on spent convictions below). This level of check is provided for duties, positions, and licenses included in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975, for example, court officers or prison employees.
- **Enhanced check.** This contains the same PNC information as the standard-level certificate but also includes a check of information held by police forces that is reasonably considered to be relevant to the position. It is available for specific duties, positions, and licenses included in both the Rehabilitation of Offenders Act 1974 (Exceptions Order 1975) and the Police Act 1997 (Criminal Records) regulations, including regularly caring for, training, or supervising children; specified activities with vulnerable adults; and applicants for gaming and lottery licenses.
- **Enhanced with a barred list check.** In addition to PNC checks, the DBS also keeps "barred lists" of people who are not permitted to work in a regulated activity with children and/or vulnerable adults. This type of certificate checks both PNC information and the barred lists and is available only for individuals carrying out regulated activity and a small number of positions listed in Police Act 1997 (Criminal Records) regulations, for example, prospective adoptive parents and taxi licenses.
- **DBS adult first check.** This certificate allows employees to start work, under supervision, with vulnerable adults before a DBS certificate has been obtained.

Under legislation, some convictions, cautions, reprimands, and warnings become spent after a certain period, meaning they do not usually need to be disclosed in background checks. Table 4.5 sets out records that must be disclosed in background checks.

Table 4.5. Information Required to Be Included in DBS Certificates

Cautions relating to an offense from a list agreed to by Parliament[a]
Cautions given less than 6 years ago (where individual is 18 or over at the time of caution)
Cautions given less than 2 years ago (where individual is under 18 at the time of caution)
Convictions relating to an offense from a prescribed list, which are serious, relate to sexual or violent offending, or are relevant in the context of safeguarding[a]
Where the individual has more than one conviction offense, all convictions will be included on the certificate (no conviction will be filtered)
Convictions that resulted in a custodial sentence (regardless of whether served)
Convictions that did not result in a custodial sentence, given less than 11 years ago (where individual is 18 or over at the time of conviction)
Convictions that did not result in a custodial sentence, given less than 5.5 years ago (where individual is under 18 at the time of conviction)

SOURCE: DBS (n.d.).
[a] For more information on these cautions, see Gov.uk (2018).

Other Criminal Records Checks

ACRO Criminal Records Office issues criminal-history certificates on behalf of most UK police forces. First, an individual who is seeking a visa to enter certain countries may be obliged to apply for a police certificate, which details whether the applicant has a criminal record in the UK (other than Scotland) and may also include foreign criminal-history information where it has been disclosed to the UK.

Second, an International Child Protection Certificate (ICPC) is a criminal record check for UK nationals or non-UK nationals who have resided in the UK who wish to work with children overseas. The ICPC is a joint initiative of the National Crime Agency's Child Exploitation and Online Protection Command and entails not only a review of criminal-history information in the PNC but also police intelligence databases, which may hold information indicating that the person should not work with children. The Child Exploitation and Online Protection Command assesses that intelligence and determines whether to issue an ICPC based on that intelligence. The certificate contains a person's complete conviction history in the PNC, including spent and unspent convictions. The ICPC also contains foreign criminal-history information that has been disclosed to the UK.

Subject Access

Individuals who are seeking to learn what information is held about them on the PNC may apply to the ACRO Criminal Records Office for a subject access disclosure. ACRO provides these disclosures from the PNC on behalf of most police forces in England and Wales, as well as Northern Ireland, Jersey, the Isle of Man, and the BTP.

E&W 3. Addressing Criminal-History Data Quality and Completeness

E&W 3.1 Procedures to Assess and Ensure Information Accuracy and Completeness

Data Quality Assurance Processes

There are numerous processes and methods by which the accuracy and completeness of the PNC data are monitored by relevant stakeholders at each stage of the data flow. As a matter of practice, while prosecuting agencies are authorized to create records and update records on the PNC, it is almost always the police who enter data into the PNC. This is because only the police have access to fingerprint records, which is generally the only way to prove the identity of an individual in the system. Fingerprints are critical to how the PNC operates and are particularly important in cases of duplicate records. Police can run a fingerprint check within 7 minutes; by comparison, a DNA test to check an individual's identity can take up to 40 days to be completed. Where no fingerprint records exist, police can also resolve issues by authenticating records with images of the individual's signature.

Furthermore, when a PNC record is being created or updated, almost all fields in a record have triggers that can alert the data entry officer that required information has not been inputted. Information on an individual's identity in their record can be overridden when errors or new information come to light, as can any warnings about the individual, for example, that they are at risk of self-harm. Police are also responsible for ensuring that PNC records are updated with court data. Almost all courts can connect to a portal that transmits outcomes to the PNC. If the update has not been transmitted successfully because of an issue in matching the information in the court update with the relevant PNC record, a notification is automatically added to what is called an exceptions report. This report, which is produced daily, is sent to the police force from which the court matter originated, which manually corrects any errors, before the update is resubmitted to the PNC.[61]

In addition, all police forces are obligated to have a PNC force lead whose responsibilities include auditing the entry and use of the data by that force. There are four main types of audit regularly conducted by the force lead: data quality in relation to PNC records created or updated by that force, compliance with PNC regulations, purpose of use, and integrity. Records can also be reviewed spontaneously, for example, during an investigation. However, police forces may not always have the resources for a dedicated member of staff to audit the force's data entry and access, which may put the quality of their data at risk. Police forces in England and Wales have a high degree of autonomy in how they allocate their resources and, in times of increasing budgetary pressures, may decide not to prioritize ensuring data quality.

HMICFRS has the authority to inspect and monitor the 43 territorial police forces in England and Wales, including their use of the PNC. HMICFRS audits police forces on their use of the PNC and compliance with the PNC code of practice.[62] HMICFRS is also authorized to audit the use of the PNC by ACRO Criminal Records Office and nonpolice agencies with access to PNC data.

Finally, nonpolice agencies with access to the PNC (e.g., the Ministry of Justice) have reported that they inform the relevant police forces when errors or inaccuracies are discovered during their use of the data, as the issues arise.

The Home Office Transformation Programme

The Home Office is currently managing a program of work called the National Law Enforcement Data Programme. The program started off with the ambition of replacing PNC. However, it was concluded that such a project would be overwhelming in complexity and required resources, particularly as changes to PNC affect every part of police business. Instead, both the PNC and the Police National Database will be replatformed, with the goal of making the

[61] According to information provided by the PNC bureau, all matching errors are successfully resolved during the manual stage.

[62] An inventory of HMIC audits of PNC audits can be found at HMIC (n.d.).

interface more intuitive and user-friendly to operate. The program intends to build the platform alongside the existing ones and can ultimately begin to transition onto the new platform in a protected way, still allowing users to have access to PNC data. The program is in the process of finding a supplier to implement this transformation.

E&W 3.2 Limitations of the Use of Police National Computer Data for Operational Purposes

Most of the limitations around using the PNC reported by interviewees relate to its relatively advanced age.[63] Several interviewees described the system as not very user-friendly and noted that the interface makes it difficult for an inexperienced user to understand how the information is displayed or where certain information within a record is held. Two interviewees also reported that the design of the platform, which was originally intended to be a basic administrative database, does not lend itself to modern use of the data set, for example, utilizing advanced data science analytical processes. To that point, one interviewee stated that police forces have requested that the Ministry of Justice, which houses an extract of the PNC in a relational database (described in Section E&W 4.2 below), run analyses of PNC data for operational purposes on their behalf, as the design of the PNC precludes more complex data analyses. Two interviewees also reported that the limitations of the technology affect how much data can be shared operationally. For example, only recent offending records may be available to a police office or offender management organization, as extracting the individual's whole offending history may be too time consuming for operational needs. One interviewee also commented that PNC is labor intensive to operate, and with increasing financial constraints on police forces, some agencies find it challenging to staff it appropriately.

One interviewee also noted that issues with mapping data between the PNC and court systems (explored in Section E&W 3.1 above) can be partially explained as a result of the court systems, which are themselves relatively dated, interacting with the antiquated technology of the PNC. Issues with police information and communication technology (ICT) beyond the PNC itself also pose challenges for its effective use. Each of the police forces in England and Wales are responsible for purchasing their own ICT equipment. Approximately 29 of the territorial police forces of England and Wales use a record management system called Niche; however, there are multiple versions of Niche in use across forces. Other forces use other commercially available systems or have created their own systems. As a result, there is no common approach to case management or feeding in data from local police systems to the PNC. Furthermore, there is no automatic link between Niche and the PNC, so users must update such information as arrests and bail decisions manually. There is currently a project aimed at moving all police forces onto the same version of Niche, although one interviewee commented that this is a complex and likely

[63] There are no official statements on this topic identified by RAND. For that reason, this section builds on testimonies of interviewed key informants.

lengthy process. Importantly, data codes are consistent across police forces, which aids in understanding and analyzing PNC records.

Feedback from interviewees about the coverage of data in the PNC was generally positive, although a few issues were flagged. Key strengths of the PNC's coverage were related to its geographical and temporal reach: data are available from all police forces in the UK, and the system has been updated electronically since 1974. Where a pre-1974 record exists on microfiche but has not been entered into the PNC, the relevant individual has a marker on their PNC record indicating that such a record exists; the PNC bureau, which sits under the NPCC, can access the microfiche and update the PNC record on request. Furthermore, since 2006, criminal records must be retained until the individual's 100th birthday, increasing the likelihood that the full history for an offender is available. However, prior to 2006, eligible records were not systematically deleted by police. As a result, there is inconsistency in pre-2006 records still retained in the PNC, and an offender's pre-2006 criminal history may or may not be complete. Criminal-history information relating to juvenile offenders is also retained in the PNC until the individual's 100th birthday.[64]

Interviewees were generally positive about the accuracy of the records contained in the PNC, and, as noted above, four interviewees attributed this to links between PNC records and biometrics. Furthermore, PNC records are updated daily, so records are likely to be current and accurate. However, three interviewees noted that some fields within records are generally more accurate than others. For example, PNCID numbers, gender, caution dates, disposal codes, length of custody, and dates of birth are considered generally accurate, but names (particularly foreign names) may be misspelled during data entry. In addition, concerns have been raised in HMIC audits of crime-recording practices in the police, particularly with reference to the underreporting of crime. However, these problems have not been attributed to issues with the PNC itself but rather a lack of training, poor supervision, and the workload of officers responsible for recording crimes.[65]

E&W 4. How Are Police National Computer Data Used for Research Purposes?

E&W 4.1 Procedures to Access Police National Computer Data for Research Purposes

Researcher Access

Historically, researchers seeking to access PNC data would apply through the PIAP for approval, detailing the data set required and including a business case arguing that a valid and lawful requirement exists for access to the PNC. However, this process has been changed with

[64] Disclosure rules for juvenile offenders are set out at Youth Justice Legal Centre (2015).

[65] More information on HMIC audits of crime-recording practices can be found in HMIC (2014).

the introduction of the MIAP, which has been granted permission from the police to house a nonanonymized extract from the PNC. This extract contains information on convictions but not on arrests and charges. While the applicant must still approach the PIAP for access to PNC data in the first instance, the application is now transferred to the MIAP for a decision on granting access. This extract is updated weekly and may be used only for research and analytical purposes by researchers within the MOJ and approved third parties, such as academics, students, or other government agencies. The data contained in this extract are at the individual level and are most commonly used to evaluate specific interventions or conduct research studies on such topics as recidivism rates.

When the MIAP receives an application from the PIAP (on average three or four a year), the MIAP must verify that the request complies with the eight principles set out in Schedule 1 of the Data Protection Act 1998 (Information Commissioner's Officer, n.d.), that the proposed research offers a demonstrable benefit to the MOJ in terms of generating knowledge, and that the data will be used for statistical and research purposes only. The MIAP will also conduct a privacy impact statement for the project. If approval is given, the MIAP creates a data-sharing agreement using a standard template that is then tailored for the specific research project. An agreement would typically contain a summary of the research project, specify the data variables the researcher seeks and provide justification for access to these variables, set out the legal basis for the application, and include terms on information security requirements and accreditation and details of the retention and destruction plan. The MIAP does not allow for the indefinite retention of PNC data by researchers. When the data-sharing agreement has been set up, the researcher will send MIAP information on the individuals for whom they require criminal-history data, such as full name, PNCID number, date of birth, and gender. The MIAP will seek to match this information with the PNC extract and share with the researchers the data they have been able to match.

The MIAP has also recently received approval to create the Microdata Lab, which is a data set from the PNC housed on a stand-alone computer within the MOJ. If researchers successfully apply for access to the lab, they can come into MOJ premises and access the entire PNC (with names of individuals redacted) themselves.

Finally, researchers who have developed a professional relationship with a police chief officer and who are seeking to conduct a research project that is deemed useful to that police force have been able to request access to the PNC records of specific individuals (not just those records created by that force) through that chief officer and do not need to go through the MIAP process.

E&W 4.2 Possibilities and Limitations of the Use of Police National Computer Data for Research Purposes

As the PNC is essentially an administrative database on a relatively old operating system, researchers cannot run any analyses through the PNC itself. Instead, the MOJ transforms the

PNC extract they receive into something that can be used for analysis by using an air gap system and running an SQL code (a standard language for storing, manipulating, and retrieving data in databases) to set up a relational database, which allows them to search and analyze the data effectively.

Even with using the MOJ database, researchers are still affected by many of the same issues around data quality as any other users of the PNC and have developed strategies to mitigate the impact of these discrepancies. As noted above, some fields within records, such as PNCID numbers, are generally more accurate than others. For example, the MOJ attempts to capture all relevant individuals when matching records from the research application to the PNC extract by using soundexing—a phonetic algorithm for indexing names by sound. Furthermore, some fields are never used by researchers as they are too problematic, for example, the field containing information on offenses committed while the individual was on bail. They saw a massive reduction in records of this type of offending in 2008 but discovered that the reason behind this drop was a change in recording practices—police now record this information in the local recording systems instead of the PNC—rather than a true reflection of reoffending behavior.

Researchers generally benefit from the coverage of data contained in the PNC (explored in Section E&W 3.2). In particular, the decision in 2006 to retain all criminal-history records until the individual's 100th birthday enables the investigation of long-term trends and changes in offending behavior. However, issues around inconsistent retention of pre-2006 records means that older criminal-history information has been removed from the PNC or improperly retained. This must be considered when using and interpreting analyses from the data.

5. Germany

Key Findings

- Germany has three national criminal-history information systems:
    - Bundeszentralregister (BZR): Federal Central Criminal Register
    - Zentrales Staatsanwaltliches Verfahrensregister (ZStV): Central Register of Criminal Proceedings
    - Bundeskriminalamt (BKA) data: federal criminal police office databases.
- Of these three systems, only the BZR holds information on court convictions and can be used for research on individual criminal histories.
- The law does not permit links between BZR, ZStV, and BKA data.

Findings on the Bundeszentralregister

- The BZR is the main database holding criminal-history information in Germany. It is the sole data source on court convictions.
- The BZR is organized in two parts (adult and juvenile) with different rules for data retention and access.
- Public prosecutors and courts discontinue a large number of cases prior to conviction. Case disposals involving adult suspects are never entered into the BZR but are included for juvenile cases.
- The BZR does not hold biometric identifiers. Criminal-history data on an individual are linked together based on his or her name and other identifiers.
- Authorities provide information to the BZR via a unified electronic reporting interface.
- BZR data are subject to quality assurance by the Federal Office for Justice (BfJ).
- BZR adult records can be accessed by
    - criminal justice and other government agencies for operational purposes
    - researchers
    - public institutions (e.g., the Parliament or Ministry of Justice) for legislative purposes
    - individuals who wish to check their own records or who request a certificate of conduct (from their records) for employment purposes.
- Access to juvenile records is more restricted.
- Access to the BZR for research purposes requires a formal application from a German university or research institute.
    - On average, the BfJ receives one application per month and approves the majority of them.
- Using the BZR for operational and research purposes is limited by expungement rules, which require that a large number of records (typically first-time minor offenses) are deleted after a limited period (minimum retention period is five years).

Findings on the Zentrales Staatsanwaltliches Verfahrensregister and Bundeskriminalamt data

- Both systems hold data pertaining to criminal investigations for use (almost exclusively) by criminal justice agencies. They do not hold data on court convictions, but the ZStV holds data on acquittals and dismissals for a limited period.
- Data quality depends on the originating agency, with no centralized quality assurance system.

DEU 1. Overview of the Country and Criminal Justice System

DEU 1.1 The Political and Constitutional System

The Federal Republic of Germany is a member of the EU with an area of 357,020.79 square kilometers and a population of about 83 million (Statistisches Bundesamt, 2019a).[66] It is a federal republic consisting of 16 federal states (*Länder*). According to the German constitution (Basic Law, or Grundgesetz), the states are endowed with their own powers and have important competencies and responsibilities, especially in education and cultural policy. They hold responsibility for local government law, police, and the implementation of federal legislation. The federal government exercises its legislative powers to create uniform civil and criminal law and civil and criminal procedural law.

DEU 1.2 Criminal Code and Procedure

Germany's unified criminal code (Strafgesetzbuch [StGB]) dates back to 1871 and has been subject to considerable revisions since its introduction.[67] There are two types of criminal offenses in Germany: misdemeanors (*Vergehen*) and crimes (*Verbrechen*). Crimes are punishable by one year or more of imprisonment, while misdemeanors carry a minimum sentence of less than a year. A large number of offenses previously considered to be criminal were decriminalized in the 1970s and are offenses dealt with administratively (e.g., most traffic offenses). Since the 1970s, new crimes have been introduced (e.g., money laundering, computer fraud, stalking, and terrorist acts), and penalties for violent and sexual crimes have increased (Krehl, 2003).

Similar to criminal law, criminal procedural law is also a matter of federal legislation (Strafprozessordnung [StPO]). German criminal procedure is fundamentally marked by the principle of legality[68] and traditionally by the principle of mandatory prosecution, with the role of punishment reserved for the courts. However, the ability of public prosecutors to end cases on their own discretion has broadened in the last few decades.

DEU 1.3 Court Dispositions and Penal Sanctions

Under general (i.e., adult) criminal law, fines and prison sentences are the main forms of punishment.[69] Prison sentences of up to two years may be suspended on probation, which can be combined with conditions on the sentenced individual (e.g., a fine or community service) or

---

[66] See Roxin, Arzt, and Tiedemann (2014) and Jehle (2010) for further information on topics addressed in this section.

[67] See Roxin, Arzt, and Tiedemann (2014), Jehle (2010), and Jehle (2015) for further information on topics addressed in this section.

[68] The principle of legality typically refers to a requirement that a person can only be held criminally responsible and punished for action that was subject to a criminal statute when the action was undertaken (nullum crimen nulla poena sine lege). For a more detailed discussion on related concepts, see, for example, Dubber (2013).

[69] See Roxin, Arzt, and Tiedemann (2014) and Jehle (2015) for further information on the topic addressed in this section.

instructions affecting the person's conduct (e.g., supervision by a probation officer). Generally, the preconditions for the decision to suspend a sentence on probation are stricter for longer prison sentences.

In addition to the sanctions mentioned above, the court may impose other measures with the aim of reforming the offender or protecting the public. Such measures include commitment to a psychiatric hospital or substance-misuse treatment, preventive detention (postimprisonment), supervision of conduct, revocation of a driver's license, and a ban on certain occupations, such as holding public office.[70] These measures may be imposed even if the person is found not guilty on the grounds of a lack of criminal responsibility.

With respect to juvenile offenders (aged 14 to 17) and young adults (aged 18 to 20) convicted under juvenile criminal law, the objective of the criminal justice system is to educate the offender.[71] To that effect, the law provides for two types of special sanctions. The first type are educative and disciplinary measures; and the second is imprisonment with the possibility of suspension and probation. Youth imprisonment is the only criminal punishment available under the Act on Juvenile Courts (Jugendgerichtsgesetz [JGG]). There are also differences between adult and youth imprisonment rules. Notably, the length of imprisonment for individuals sentenced under juvenile criminal law is limited to between six months and ten years.[72] Children aged 13 or younger are not held criminally responsible.

DEU 1.4 Agencies in the Criminal Justice Chain and Their Role

Law enforcement: Police under the direction of the prosecution service are responsible for investigating the majority of criminal offenses.[73] Each of the 16 federal states has its own police force. Cooperation between state-level agencies is coordinated by the BKA, which handles the most serious investigations, such as terrorism and organized crime. Police must provide the results of their work to the public prosecution office; police have no discretion to discontinue a criminal case. According to the StPO, while provisional arrests are used only in a small number of instances, police and public prosecution offices are authorized to make a provisional arrest if

---

[70] Preventive detention (postimprisonment) (*Sicherungsverwahrung*) refers to the possibility of holding an individual detained after the completion of the sentence on the grounds of the individual's continued dangerousness and likelihood of committing new crimes (in accordance with § 66 StGB). It is usually imposed before imprisonment as part of the same conviction. See Janus et al. (2012).

[71] Young adult offenders are required to be processed under juvenile criminal law if they are considered to be juvenile in terms of their development or if the offense was a transgression of a juvenile nature. If this does not apply, they are dealt with under general criminal law. In 2017, juvenile criminal law was applied in 64 percent of all convictions against young adults (excluding traffic offenses) (Statistisches Bundesamt, 2018b).

[72] By contrast, the length of imprisonment under adult criminal law ranges from 1 month to 15 years, with life sentences possible in exceptional cases. The juvenile criminal law foresees the possibility of a 15-year sentence for a murder with an especially aggravated amount of guilt (§105 (3) JGG).

[73] See Roxin, Arzt, and Tiedemann (2014) and Jehle (2015) for further information on topics addressed in this section.

the prerequisites for a court's order of pretrial detention (remand custody) have been fulfilled.[74] Police must bring the suspected person before a local court judge as soon as possible within one day after the provisional arrest. If the judge does not order pretrial detention, the suspect will be released.

Prosecutors: Public prosecution offices are organized parallel to the courts and are responsible for bringing charges against suspected persons.[75] However, under certain conditions, they may decide to discontinue the case. For instance, the public prosecution office terminates the case if no suspect is found, if there are no sufficient grounds for suspicion, or if the accused's guilt is of a minor nature and there is no public interest in prosecution. Examples of this last category include first-time shoplifters or possession of a small amount of marijuana for personal use. Further, the public prosecution office can terminate the case under certain conditions, such as payment of money to a charitable organization or to the state, with the approval of the court and the suspect's consent.[76] In the remaining cases, the public prosecution office charges the suspect or applies for a penal order from the competent court.[77] The public prosecutor can apply to issue an arrest warrant, order of pretrial detention, or remand custody by the judge of the local court, usually after a provisional arrest made by police. Special arrangements apply to criminal proceedings against juveniles (aged 14 to 17) and young adults (aged 18 to 20).

Courts: On the filing of charges by the prosecutor, the court examines why the accused is suspected of the offense and whether these reasons are sufficient for the court proceedings to begin. In most cases, the court of first instance is the local court (*Amtsgericht*). If the offense is a misdemeanor likely to result in a sentence of no more than two years of imprisonment, one judge will preside over the case. If the offense in question is likely to result in a sentence of two to four years of imprisonment or if the offense is a crime (*Verbrechen*), the case will typically be heard by a judge joined by two lay judges (*Schöffengericht*). More serious cases are dealt with by the regional court (*Landgericht*). Specifically, a regional court's grand criminal chamber (*Große Strafkammer*) hears all cases that are expected to result in any of the following outcomes: (1) imprisonment longer than four years, (2) commitment to a psychiatric hospital, (3) imposition of preventive detention (postimprisonment). Special juvenile courts hear cases against juveniles and young adult offenders. The chamber consists of two to three professional judges and two lay judges.

---

[74] Although the number of recorded crimes is known, there are no data available on the number of arrests made by police. Data are collected only on the number of persons held on remand (i.e., after their pretrial detention has been approved by a judge).

[75] See Siegismund (2003).

[76] Examples of applicable conditions are listed in §153a StPO.

[77] Applications for penal orders consist of a simplified procedure (involving no oral proceedings) that can be used for noncomplex cases. Penal orders cannot be used for crimes (*Verbrechen*), and the range of sanctions that can be imposed is limited.

DEU 1.5 Size of Criminal Justice System

Figure 5.1. illustrates the law enforcement process and provides an overview of the scale of the German criminal justice system.[78] The figure shows all offenses except traffic offenses (which are not included in police crime statistics) for 2016.

In 2017, there were approximately 5.8 million recorded offenses, corresponding to a crime rate of nearly 70 crimes per 1,000 population. More than half (about 3.3 million) of offenses were cleared, and about 2.1 million suspects were identified.[79] The number of persons whose cases were decided in court in 2016 (approximately 700,000) was substantially lower than the number of alleged offenders identified by police. Several possible reasons account for the difference between the number of identified suspects and court decisions. These reasons include cases being terminated (e.g., due to insufficient evidence or the insignificance of the offense), the existence of more than one set of criminal proceedings against a given person, or other disposals by the public prosecution office. Most of the sanctions imposed in court are fines or, in the case of juveniles and young adults, educative or disciplinary measures. A small minority are given a prison sentence, and most sentences of this kind are suspended with the offender being put on probation. Altogether, 5 percent of convicted persons are sentenced to serve an unsuspended prison term.

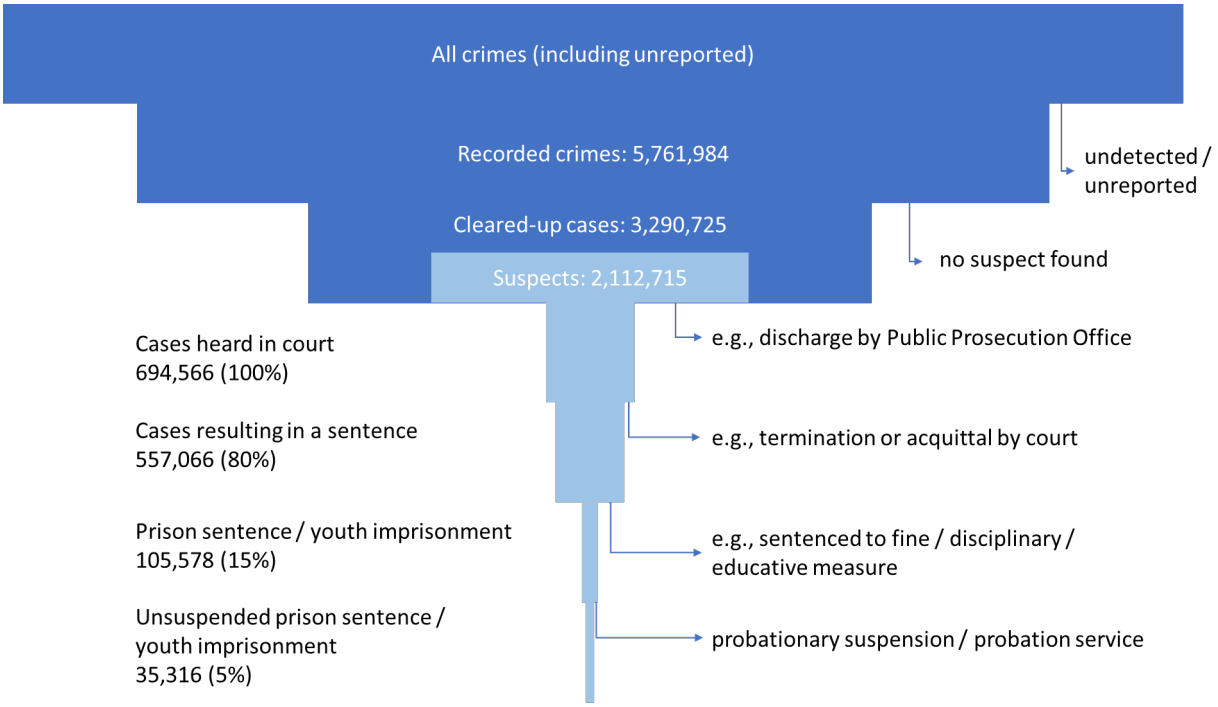
As of November 30, 2018, a total of 63,643 persons were imprisoned in Germany, at an incarceration rate of 76.7 per 100,000 persons. Seventy-six percent of prisoners were serving a prison sentence, and 22 percent were in remand (pretrial) custody. Prisoners detained for other reasons (e.g., those in custody awaiting deportation) accounted for approximately 2 percent of the prison population.[80]

[78] See Jehle (2015), Bundeskriminalamt (2019), and Statistisches Bundesamt (2018) for further information on topics addressed in this section.

[79] This number refers to individuals identified by police as alleged perpetrators. It could include individuals who are deceased or at large.

[80] See Statistisches Bundesamt (2019b).

Figure 5.1. Overview of the German Criminal Law Enforcement Process (Excluding Traffic Offenses), 2017



SOURCE: Bundeskriminalamt (2019) and Statistisches Bundesamt (2018a).
NOTE: Figure format based on a figure provided in Jehle (2015); updated with 2017 data and labels modified by the authors.

DEU 2. Bundeszentralregister

DEU 2.1 History and Organizational Management

The main database holding criminal-history information in Germany is the Federal Central Criminal Register (BZR).[81] The BZR is the sole data source on court dispositions and individuals' full criminal history (i.e., including convictions) in Germany.[82] In addition to the BZR, two other information systems hold information on persons who come in contact with the German criminal justice system: the ZStV, a register of criminal proceedings, and databases managed by the BKA. Both are used exclusively during the course of criminal investigations, and neither contains information on court convictions (although the ZStV holds data on acquittals and dismissals for a limited period). Because this report focuses on national-level criminal-history systems, the remainder of the chapter discusses the BZR. Information on ZStV and BKA files is presented in Appendixes DEU A through C.

[81] In addition to expert input and applicable legislation, references relevant for Chapter 5 include Morgenstern and Arndt (2011), Jehle (2015), and Tolzmann (2015).

[82] Dispositions other than convictions are not recorded, with the exception of cases tried under juvenile criminal law.

The BZR is a centralized stand-alone repository of criminal records in Germany. It was set up in 1972 after the Federal Central Criminal Register Act (Bundeszentralregistergesetz [BZRG]) came into force. The BZR replaced criminal registers of the 93 regional prosecution offices maintained by individual federal states.[83] The BZRG is the governing legislation for the register and determines such fundamental arrangements as what data can be held and for how long and who has access.

Following the adoption of the BZRG, further legislative and administrative changes have affected the register. As a general rule, all legislative changes concerning criminal offenses or penal sanctions are reflected in the register, including permanent amendments of the database as necessary. Recent modifications include the following:

- In 2007, the operation of the register was taken over by the Federal Office of Justice (Bundesamt für Justiz [BfJ]). Previously, this role was performed by the Federal Prosecution Agency (Generalbundesanwalt).
- Starting in 2009, all employers whose work involves children and young persons (e.g., child care and youth welfare agencies) are required to check employees and job applicants against the register. The BZRG was amended accordingly.

As of 2018, the BZR held records on approximately 4.3 million individuals with 16 million court dispositions.[84]

DEU 2.2 Content

The BZR is organized in two parts (adult and juvenile). The adult part is called the Central Register (Zentralregister) and includes the following information:

- all convictions of German courts and judgments of foreign courts against persons with German citizenship and persons living in Germany, except educative measures according to the Act of Juvenile Courts, but including juvenile prison sentences; adult court cases that do not result in a conviction (i.e., those dismissed by the judge or resulting in acquittal) are not recorded[85]
- rulings of administrative authorities (e.g., revocation of a business license, prohibition of certain professional activities, suspension of a passport, or revocation or rejection of a weapon permit)
- judgments that a person lacks criminal capacity due to mental illness
- follow-up developments related to the execution of the sentence (e.g., early release, parole, revocation, or suspension of a penalty)
- warrants of apprehension that can be recorded.

[83] See Morgenstern and Arndt (2011).

[84] According to unpublished internal reports.

[85] According to 2017 data, juvenile prison sentences are imposed in approximately 17 percent of all convictions according to the juvenile criminal law (excluding traffic offenses) (Statistisches Bundesamt, 2018b).

The juvenile part is called the Register of Educative Measures (Erziehungsregister, henceforth Educative Register) and includes the following information:

- disposals of public prosecution according to the Act of Juvenile Courts (with or without the imposition of a condition)
- educative measures imposed by a juvenile court.

Central and Educative Register files are similarly structured and contain the following information:

- personal information, including name(s) and aliases, sex, address, nationality, and date and place of birth[86]
- name of the deciding authority
- date of offense
- date of judgment, appeals, and date of judgment's entry into force
- legal description of the offenses, including relevant norms of the StGB
- details of the measure or penalty imposed (e.g., length of prison sentence, its suspension, length of probation and appointment of probation officer for suspended sentences, and amount and length of fines); if total penalty is composed of multiple individual penalties, the total will be registered
- suspension of driving license, if applicable
- where applicable, information related to drug dependence, including information on detention in a rehabilitation clinic and if the offense was committed as a result of drug dependence (if the sentence is for less than two years).[87]

The BZR is a name-based system and does not include any biometric information.

Courts and other relevant authorities must report information to the BZR within one month of the date of the conviction.[88] Data must be transferred electronically in a unified form via the automatic notification and information procedure (*automatisches Mitteilungs- und Auskunftsverfahren*). Authorities report data in a standardized electronic form consisting of mostly coded fields and some text fields (e.g., offense description). Encrypted files are transferred over a federal government-run network (Deutschland Online Infrastruktur [DOI-netz]).[89] Authorities do not gain direct electronic access to the database when they report information to the BZR; only BfJ personnel have this access.

Local authorities responsible for the registration of residents (*Meldebehörden*) automatically report name changes. If the person of interest has a record in the register, it will be updated accordingly.

---

[86] Unlike some other EU countries, there is no national identification number in Germany.

[87] Pfeiffer (2000) noted this as a possible source of errors, with drug-related information not recorded properly. A possible contributing factor may be the fact that this type of data may not be easily accessible from court data, which form the basis of the BZR record.

[88] Details are specified in a general administrative regulation. See Tolzmann (2015, p. 104).

[89] See BfJ (n.d.a).

Deletion from the Central Register

The rules for retention of records in the BZR aim to rehabilitate sentenced persons and reflect a principle that offenders should generally not be known as punished persons for the entirety of their lives. Rather, after a certain period without criminal behavior, there should be no public knowledge of their criminal history.[90] However, records are retained for longer periods for more severe sentences and are not deleted until the person's death or advanced age for repeat severe sentences.

In general, records can be deleted from the register under one of three types of circumstances: automatic deletion, conditional deletion, or deletion on application.

Automatic deletion: Entries are automatically deleted from the Central Register in the following cases:

- three years after the official notification of the person's death[91]
- after the individual in question reaches age 90
- for court dispositions for entries that relate to lack of criminal responsibility due to a mental illness:[92] 20 years after the decision for crimes and 10 years for misdemeanors (extended to 20 years for misdemeanor cases involving sexual offenses).[93]

However, no automatic procedure exists to verify that the criteria for automatic deletion have been met. Instead, the process is triggered on an ad hoc basis. As a result, the BZR holds numerous records that should be deleted but are not (e.g., deceased persons).

Conditional deletion: Entries in the Central Register can be deleted after the expiration of a certain period if the person does not receive any new convictions. The length of time after which records are deleted is determined by the sentence in question. Germany uses a graduated approach whereby more serious sentences or offenses will generally be associated with a longer retention period. Life sentences, preventive detention, and mental hospital orders represent exceptions and are not eligible for conditional deletion from the Central Register.

Criminal records that are eligible for conditional deletion are subject to four distinct retention periods, depending on the sentence in question (see Table 5.1). The retention periods were determined as part of the BZRG legislative process. Germany applies a principle of unity of the criminal record. This means that if the person has multiple convictions that may be subject to

---

[90] See Morgenstern and Arndt (2011).

[91] No entities are responsible for notifying the BZR of deaths. Deaths are notified to the person's local registry office (§28ff PStG—Personenstandsgesetz, Civil Status Act). However, the registry office does not know if a person has a record in the BZR and has no obligation to inform the BZR of every death. Therefore, some records may be held longer than necessary.

[92] In cases where the offender is not considered dangerous and is therefore not sent to a psychiatric hospital or drug treatment facility (§11 BZRG).

[93] §174–180, 182 StPO.

different retention periods, no convictions can be deleted until the person's latest conviction is eligible for deletion.

Table 5.1. Bundeszentralregister Retention Period by Type of Sentence

Retention Period	Type of Sentence
5 years	Fines of no more than 90 day units if there is no other imprisonment or detention registered[a]
	Imprisonment of no more than 3 months if no other sentence is registered
	Juvenile prison sentence of no more than 1 year (or no more than 2 years in the event of suspension or parole, or more than 2 years after successfully completing parole)
	Juvenile prison sentences where the criminal stigma has been declared extinguished
	Convictions leading to additional measures, such as confiscation orders
10 years	Sentence of no more than 3 months if another sentence is registered
	Sentence of no more than 3 months but not more than 1 year followed by parole
	Juvenile prison sentences of more than 1 year because of certain violent or sexual offenses or if there is no parole
15 years	Sentences not covered by other retention periods
20 years	Sentences or juvenile sentences based on sexual offenses (§174–180, 182 StPO)

[a] Day units, day fines, or unit fines are monetary penalties that consider the economic situation of the offender (e.g., standard of living, family situation, and expenditures). For a discussion of the introduction of day fines in Germany, see Gillespie (1980).

Several additional details apply to the deletion procedure. The retention period will be extended by the length of time spent in prison or detention. Thus, the periods listed in Table 5.2 start once the individual is released from custody. The actual deletion occurs one year after the record is eligible for deletion. However, no information pertaining to this record can be provided from the BZR within this year, and the record is not visible to anyone outside of the BZR authority. This one-year period accounts for the possibility that there has been a new conviction against the person in question during the data retention period that has not yet been reported to the BZR authority by the time the formal retention period has elapsed. If any such conviction is reported to the BZR within the year after deletion, the record will be updated and retained. If no entry to the BZR is reported within the year, the record will be deleted. Once the deletion is carried out, the record is not retained in any form and cannot be recovered.

If there is a change in the law and the offense in question is no longer punishable by imprisonment, the person concerned can apply to have the record expunged. Also, if a criminal record was deleted incorrectly and the BZR authority plans to reinstate the record, the person concerned may provide a reaction to the decision to reinstate the record before it is carried out.

Deletion on application: Records can also be deleted after an application filed by the person concerned is approved or by public authorities on their own initiative. The BfJ receives about 200 such applications each year. When an application is filed, the BfJ collects statements by the involved authorities and makes a decision. By law, the deletion can only be approved if the sentence is enforced and the deletion is not against public interest. A small number of

applications are usually approved (four applications in 2016 and one in 2017).[94] If an application is denied, the applicant can file a complaint against the decision of the BfJ at the Federal Ministry of Justice and Consumer Protection (Bundesministerium für Justiz und Verbraucherschutz). If the applicant is not successful after completing that step, he or she may appeal to the appellate court of Berlin against the decision of that ministry.

Deletion from the Educative Register

Retention arrangements for data held in the Educative Register are comparatively simpler. Records are automatically deleted when the person concerned reaches age 24, unless there is a record for the same person in the Central Register. In addition, as with the Central Register, entries can be deleted on request or on authorities' own initiative.

DEU 2.4 Access to Data for Operational and Civil Purposes

Access to Central Register Data

There are two types of access to the Central Register (Table 5.2). The first type allows access to the full register and is afforded to selected institutions. No private individuals have this type of access, with the exception of individuals reviewing their own records. The second type allows access to selected information held in the Central Register and is undertaken through an instrument called a certificate of conduct (*Führungszeugnis*). The remainder of this section describes the access of BZR data for operational and civilian purposes. Access for research and legislative purposes is discussed in Section DEU 4.

Table 5.2. Types of Access to Central Register Data

Type of Access	User	Purpose	Discussed In
Access to full data	Public authorities	Operational	Section DEU 2
	Individuals	Review of personal records	Section DEU 2
	Public authorities	Legislative	Section DEU 4
	Researchers	Research	Section DEU 4
Via certificate of conduct	Individuals	Civilian	Section DEU 2

Recording of Queries

For all types of access, the BZR administrators need to record the following details about every query or notification:

- applicable BZRG provision
- purpose of the query
- personal data used in the query and response

[94] According to unpublished information provided by the BfJ.

- requestor and recipient of information
- date of transmission
- name of staff involved
- file or record number.

Administrators use the log to notify agencies in the event of simultaneous queries, internal audits, and data protection control. Log data are deleted after one year. According to unpublished BfJ data, the BZR processed 15 million requests for information in 2018.

Institutional Access for Operational Purposes

In accordance with the BZRG, the following entities have complete access to the Central Register:

- courts, public prosecution, and supervision authorities[95]
- highest federal and state authorities[96]
- secret services (domestic, foreign, and military intelligence)
- financial and tax authorities' criminal investigation departments
- criminal investigation units of police departments
- naturalization services
- state authorities dealing with foreigners and the Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge) (if a record is related to a migrant or foreigner)
- specialized administration agencies:
  - authorities granting hunting permits, dangerous dog permits, and guard or private security business inspection authorities
  - Federal Institute for Drugs and Medical Products/Devices (Bundesinstitut für Arzneimittel und Medizinprodukte)
  - lawyer and patent office chambers
  - Federal Nuclear Safety Office (Bundesamt für kerntechnische Entsorgungssicherheit)
  - air safety authorities.

In addition, Germany participates in the European Criminal Records Information System (ECRIS) and shares criminal-history information with other EU countries under this framework. The details of the system are presented in Box 1.

[95] In accordance with §68a StGB. The supervision authorities are part of the judiciary and oversee persons under supervision of conduct (*Führungsaufsicht*). These individuals include prisoners who served two or more years and detainees released from a mental hospital, addiction-treatment facility, and preventive detention (*Sicherungsverwahrung*). Probation officers involved in this supervision do not have full access.

[96] However, these authorities can pass information that is not included in a certificate of conduct (i.e., available only through full access to the BZR) to their subordinate or supervisory agencies/departments only if it is necessary to avoid disadvantages to the federal state (*Land*) or the republic as a whole (*Bund*).

Box 1. European Criminal Records Information System

ECRIS is an EU information system designed to facilitate the exchange of criminal-history information between EU member states, thereby ensuring national authorities have access to relevant criminal-history information. ECRIS was introduced in 2009 and implemented in 2012 as a decentralized information technology system.[97] Criminal record data are stored solely in national information systems (each participating country designates a competent authority); no central EU-level repository collects data from individual member states. Instead, competent authorities directly transfer data to other member states.[98] To this date, however, not all EU member states have joined the system, and participating member states have not always established connections with all other participating countries.[99]

Participating member states have an obligation to report convictions (and any subsequent updates or deletions) of nationals of other member states to their respective countries of citizenship, although not all countries comply with this requirement.[100] Member states also have the ability to request information on a given individual from other countries.[101] Member states have an obligation to respond to a request for information within ten working days.[102] When a member state receives conviction information on its own nationals from other EU member states, it is required to store that information for the purposes of future retransmission and make any updates or deletions if subsequently communicated by the convicting member state. Thus, ECRIS helps ensure that when replying to requests from other countries, member states are in a position to provide complete and up-to-date information on their own nationals irrespective of where they were convicted (Jackson and Davies, 2017).

Specifically, EU member states are obliged to provide the following information:[103]

- details on the convicted person (current and previous names, date and place of birth, gender, and nationality)
- administrative details of the conviction (date of conviction and when the decision became final, and name of the court)
- information on the offense leading to the conviction (date, name of the offense or its legal classification, and a reference to relevant legal provisions)
- contents of the conviction (the sentence applied, including any supplementary penalties, measures, and subsequent modifications to the execution of the sentence).

If included in the criminal record, the following information will also be shared by member states: the names of the convicted individual's parents, the place of the offense, the conviction's reference number, and any disqualifications resulting from the conviction. Furthermore, if a member state's competent authority possesses the convicted person's fingerprints, aliases/pseudonyms, and identity number, this information will also be shared. There is no formal requirement to share any additional information (e.g., factual details pertaining to the offense or conviction), although member states may decide to share further criminal record details as they see fit.

Information is transmitted electronically in a unified format. To accommodate variations across EU member states in the criminal justice systems, member state authorities use two reference tables with categorizations of offenses and penalties, which group all possible national offenses and penalties into a set of categories common to all EU member states.[104] Alongside the reference tables, practitioners can make use of a nonbinding manual for practitioners, intended to assist ECRIS users with the system's operations (ECRIS Support Programme, 2013).

The development of common reference tables helps ECRIS users approximate offenses and sanctions across all

[97] See Council of the EU (2009).

[98] See EC (n.d.).

[99] As of 2016, Portugal and Slovenia had not joined the system (EC, 2016).

[100] See EC (2017).

[101] ECRIS does not provide member states with automatic access to other member states' systems.

[102] The deadline is extended to 20 working days when the request is submitted on behalf of an individual asking for their own criminal record information. Per Article 8 of Council Framework Decision 2009/315/JHA.

[103] Per Article 11 of Council Framework Decision 2009/315/JHA.

[104] The common tables of offenses and penalties and measure categories are provided in the decision on the establishment of ECRIS (Council of the European Union, 2009).

EU member states. However, some potential issues remain. For example, a certain activity could be a crime in one country but not the other, leading to uncertainty over how the information would be transmitted and uploaded by the receiving country (Jackson and Davies, 2017).

Three member states discussed in this report participate in ECRIS—Germany, the Netherlands, and the UK. Their number of connections to other member states as of 2016 and number of notifications, requests, and responses to other member states in 2016 are summarized in Table 5.3. Germany is the most active EU member state in terms of new conviction notifications (30 percent) and issued requests for information (39 percent).

Table 5.3. European Criminal Records Information System Statistics for Germany, the Netherlands, and the United Kingdom

Country	Connections	Notifications	Requests	Responses
Germany	24	98,422	140,669	21,849
Netherlands	24	7,174	9,104	12,686
United Kingdom	24	32,889	97,425	13,000

SOURCE: EC (2017a).

For reasons of rehabilitation of offenders, limitations are placed on access to some information by selected institutions. Specifically, only criminal courts and prosecutors can be informed about two types of special records. First, if a person with an unsuspended prison sentence has been allowed to undergo a drug-treatment program outside of prison, this specific information is available only to criminal courts and prosecutors. Second, before a juvenile prison sentence entry becomes eligible for deletion, the juvenile prison court can decide to extinguish the so-called criminal stigma. In such situations, while the information stays in the Central Register, it is not visible for the purposes of a certificate of conduct and to authorities other than criminal courts and prosecutors. However, there are exceptions to this limitation, mostly pertaining to sexual and violent offenses.[105] In addition, requests for information from the Central Register may be rejected if necessary for witness protection.

As discussed above, no authority has direct online access to the database of the BZR. Instead, an authority must make an individual request using a unified electronic form and indicating the purpose of use. The electronic form is sent to the BZR authority via the Automatic Reporting and Information Procedure and entered into a data communication computer. The computer runs 24 hours per day and allows an automatic check and response to the request to be provided within 30 minutes, unless the request requires further analytical or technical input.[106]

Access for Civilian Purposes

Any individual aged 14 or older can make a request to see what records are held on them in the BZR. This affords individuals full access to data held by the BZR. The inspection must take

[105] As listed in §41 (3) BZRG.

[106] See Tolzmann (2015, pp. 26, 254–255).

place in a courtroom with no other individuals present, and no copies or notes can be made. These limitations ensure no one is forced to disclose their criminal history to third parties.

Civilians also can access BZR data via a certificate of conduct, typically for employment or background check purposes. The certificate plays an important role in balancing the interests of employers and employees. In support of the rehabilitation of convicted persons, only a limited section of the Central Register is reflected in the certificate of conduct. Certain first or minor sentences are not reported, and others are not included after a certain period following the completion of the sentence.[107]

Only the person concerned (aged 14 and above) or a legal representative can request a certificate, typically when applying for a job. There are two possible ways to apply. Owners of newly issued identity cards with online functionalities or holders of electronic residence permits can apply online directly to the BfJ, utilizing a card reader and a specialized application. Others must submit an application in written form through their local registry office, so the applicant's identity can be checked. The office subsequently transfers the request via the automatic notification and information procedure, and the BZR authority sends the certificate (in a hard copy version) directly to the applicant.[108] In exceptional cases, if the certificate is needed for a public authority, the certificate will be sent directly to the authority. However, applicants can ask for the certificate to be sent to them if it contains entries, in which case they then decide whether to have it sent on or destroyed.

As stated above, not all convictions will appear on the certificate. All entries into the Educative Register and all sentences not exceeding 90 day-unit fines or three months of imprisonment are excluded. The same is true for minor forms of juvenile prison sentences and suspended sentences in connection with drug addiction.[109] Concerning more serious records, with some exceptions (e.g., conditions related to a life sentence), there is a time frame for inclusion of records in the certificate of conduct.[110] This primarily depends on the sentence in question (Table 5.4) and is generally shorter than the retention period for the record itself. If an applicant has multiple convictions, as long as at least one conviction must appear on the certificate, all convictions will be listed. An extended certificate of conduct is required for jobs involving work with children; this certificate is governed by stricter rules regarding what information is included, particularly in connection with sexual offenses.

---

[107] See Tolzmann (2015, p. 147). Similarly, Morgenstern and Arndt (2011) pointed out the rehabilitative reasoning behind this arrangement as it allows more persons to claim they have a clean certificate (e.g., when applying for a job).

[108] Local offices also have the option to transmit the application for a certificate of conduct to the register authority via alternative modes of electronic communication (BfJ, n.d.a).

[109] These rules do not apply in connection with an application for an extended certificate of conduct in which the applicant has been convicted of certain offenses.

[110] Other exceptions to which the limitations on the time frame for inclusion in the certificate do not apply include the imposition of preventive detention and, in the event the certificate is requested by a public authority, mental hospital orders.

Table 5.4. Time Frame for Inclusion of Records in a Certificate of Conduct in Germany

Time Frame	Type of Sentence
3 years	Offenses that carry a maximum of 90 day-unit fines or prison sentences of 3 months (if eligible for inclusion in the certificate) Suspended prison sentence of less than 1 year Higher limits apply for juvenile sentences
5 years	Sentences eligible for inclusion in the certificate not listed under other time frames
10 years	Convictions for sexual offenses with a punishment of more than 1 year (both adult and juvenile) For the extended certificate, the list of applicable offenses is longer

For offenses with five- and ten-year time frames and juvenile sentences subject to the three-year period of eligibility, the time frame for inclusion is extended by the length of the sentence. Thus, the time frame starts running once the sentence is completed. In the case of commuted life sentences, the time frame is extended by the time between conviction and the end of probation or by 20 years, whichever is longer. For all other offenses, the period starts with the first judgment.

Access to Educative Register Data

Information from the Educative Register can be provided only to the following:

- courts, prosecution, and corrections
- family courts (for proceedings on the care of the person concerned)
- youth and juvenile offices (*Jugendamt*)
- authorities issuing weapons and explosives permits
- intelligence agencies (in some cases).

Information from the Educative Register cannot be forwarded to any other authority, including police.

The procedures involved in the logging of requests for information are the same as with the Central Register. With respect to disclosure to third parties (e.g., when asked about a criminal record by a prospective employer), individuals do not have to disclose any entries in the Educative Register. That is different from data held in the Central Register, which are required to be disclosed unless they would not appear in the certificate of conduct or are about to be deleted.

DEU 3. Addressing Bundeszentralregister Data Quality and Completeness

DEU 3.1 Procedures to Assess and Ensure Information Accuracy and Completeness

To audit the quality and accuracy of data held in the BZR, the BfJ has put quality assurance processes in place. One enabling factor for this arrangement is that, unlike with the ZStV (see DEU Appendix B), data included in the BZR are owned by the federal government and are thus controlled by a federal agency, the BfJ. When a record is submitted to the BZR, it is

automatically checked for compliance with formal requirements and plausibility (i.e., whether it is free of errors and inconsistencies). If an error is detected, the BZR will attempt to correct the mistake, and the reporting authority receives a return receipt when everything has been corrected. Errors can occur when new data are entered (e.g., a record exists for a person with the same name but different information). In such cases, the submitted record is checked and corrected if necessary. The BZR can check with other administrative bodies for the purposes of data verification if necessary.

If the BZR cannot correct the mistake, the reporting authority will receive an error report with explanations and will need to resubmit the record. If the reporting authority finds an error in its submission after it has been accepted by the BZR, the authority is required to send a corrected report.

Furthermore, if reporting authorities notice an error in an existing record in the BZR, they are obligated to notify the BZR authority. If the BZR's management notices an error themselves, they will ask for a clarification from the notifying authority. Authorities that have received incorrect information will be notified of any corrections (however, exceptions apply). If data accuracy is challenged by the person concerned, the record will be blocked from any information requests until the challenge is resolved.

In the context of a nationwide reconviction study (see below in Section DEU 4.2), the BZR data could be compared with data from national conviction statistics, which are compiled via a different independent reporting system. This double-check revealed that the number of convictions and individual types of sanctions recorded in each data set were nearly identical. Thus, this could be understood as an indication of the reliability of BZR data.

DEU 3.2 Limitations of the Use of Bundeszentralregister Data for Prosecution and Judicial Purposes

The main purpose of the BZR is to provide information on the criminal history of persons convicted or sentenced by criminal courts or handled by juvenile courts. The main users of the information are prosecution authorities (including police) and courts. There are several limitations and restrictions that may prevent these users from obtaining a complete picture of an individual's criminal history:

- **Record deletion and expungement.** Under current data retention rules, there is a lifelong record of the most severe sanctions and of repeat serious offenses. In other words, if an ex-offender is convicted of another crime within a specified period of the completion of his or her sentence, the retention period pertaining to the original record is extended. Therefore, if certain relapses occur repeatedly, entries may never be deleted during the offender's lifetime. On the other hand, entries on petty offenses leading to a fine or short prison sentence (no more than three months) will be removed if no reconviction occurs within a five-year period. As a result, petty offenses are not completely reflected in the register.

- **Limited access to the Educative Register**. The Educative Register holding juvenile justice responses (except juvenile prison sentences) is open to public prosecution offices and courts but not to the police. Consequently, police have formally no way of knowing whether the person in question has previously faced a charge in juvenile court.[111]
- **Dismissals of criminal cases by public prosecutors or courts.** Criminal cases can be dismissed by the public prosecutor or the court if the accused person committed a minor offense and there is no public interest in a prosecution. These dismissals are recorded for a limited period in the Prosecution Register (ZStV) (see DEU Appendix B) but not in the BZR. Therefore, a large number of first-time petty offenses are missing from the register. However, if an offender commits petty offenses repeatedly, they will no longer be dismissed but will result in a sentence recorded in the BZR.

Furthermore, because the BZR includes no biometric identifiers, searches are done by name. This can result in false positives, although the use of dates and places of birth as complementary search terms may mitigate the risk. This issue is of particular concern in relation to persons of migration background with very common names.[112] Not all countries have a working nationwide registry system. Therefore, important data (such as the date of birth) are unknown, often to the persons themselves. In those cases, the registry offices in the respective countries regularly use January 1 as the date of birth. In instances where individuals have common first and family names and only a province given as birthplace, the personal record contains data that can be common to multiple individuals. There is also a risk of false negatives, particularly with respect to individuals whose names may not have been transliterated into the Latin alphabet in a consistent manner by all reporting authorities.

DEU 4. How Are Bundeszentralregister Data Used for Research Purposes?

DEU 4.1 Procedures to Access Bundeszentralregister Data for Research Purposes

Access for Legislative Purposes

The BZR authority can transmit information from the register in an anonymized form to public authorities if needed to prepare or evaluate legislation or other legal rules. This is a rare type of request, occurring on average no more than once or twice per year. In these cases, the Federal Ministry of Justice explains to the BZR authority what data are needed, possibly accompanied by Excel templates to be filled in. The BZR authority then sends the requested data to the ministry as soon as possible.

---

[111] Despite this limitation, the police may still hold some information on the individual in their own files, for instance, if the individual had interacted with the same police station. Furthermore, the police may have information on any judicial proceedings against the person if a police officer appeared in court as a witness.

[112] According to the German Statistical Office, a person is of migration background (*Migrationshintergrund*) if "they or at least one of their parents are not German citizens by birth." See Statistisches Bundesamt (2017).

Typically, requested data are simple tables or lists and anonymized data or frequencies of certain entries. The BZR authority itself compiles and analyzes data needed from the register, or a research institution is commissioned to analyze data delivered from the register.[113] For example, in 2016, the German federal government commissioned a research institute to evaluate a new type of juvenile detention introduced into the Juvenile Court Act and in particular to analyze reconviction rates after this measure entered into force.

Researcher Access

Provisions also exist for access to the BZR for research purposes, in both anonymized and nonanonymized forms.[114] In accordance with §42a Sec. 1 BZRG, the BfJ can transmit nonanonymized data from the BZR to universities or other research institutes under the following conditions:

- The data are needed for a research project.
- The use of anonymized data is not possible.
- The public interest in the research outweighs the interests of the persons concerned.[115]

BZR data are typically used for two types of research. First is research of criminal-history records of offenders, prisoners, and detainees to examine the effect of the sentence or of treatment programs, using reconviction after release as an outcome variable. Under this scenario, researchers will give names to the BZR authority and receive data from the register about those individuals. Second is research of persons, without searching for specific names, who have received a particular type of sentence or have been released from a certain form of detention or prison. One example is the study of all sex offenders released from a psychiatric hospital in 2012 and their reconvictions until 2016. Under this scenario, researchers can obtain the information either in the form of anonymous statistical data, or, if researchers want to also examine the criminal case files of the persons concerned, they can obtain the full person-related data, including the reference number of the criminal files.

To obtain access to data, researchers submit a proposal outlining the research project and the need for BZR data. In particular, the application needs to specify why personal data are needed (if applicable) and why the public interest represented in the research project outweighs the personal rights of the persons whose data are concerned. The proposal also needs to specify the precautions used to protect personal data and to present details on the researcher and the institution. The register authority assesses the completed application, checks whether all prerequisites are met, verifies that data protection and security are guaranteed, and examines the

[113] See Tolzmann (2015, p. 260).

[114] As stipulated in §42a BZRG, the procedures for access to the Educative Register for research purposes and for the logging of requests for information are the same as those for the Central Register.

[115] See Bundesministeriums der Justiz und für Verbraucherschutz (2017b).

application for any flaws or missing information. The register authority will then discuss any resulting questions with the applicant.

To date, requests for BZR data have been granted only to German researchers because the register authority cannot control data protection agreements and facilities in other countries. In this regard, applications need to have the backing of an established research institute or university.

From 2001 to 2017, the BfJ received 211 research applications, averaging approximately 1 per month (Table 5.5).[116] The request for information was granted in more than 70 percent of the cases. Nearly 2 percent of the cases are still open and can lead to eventual provision of information. For the majority of cases where the BZR authority did not provide information, applicants did not follow up on their requests or withdrew the requests (12 percent of total applications). Further, 12 percent of the applications were rejected; in 1 percent of the cases, applicants were redirected to other sources of information, which eliminated the need for BZR data (Götting, 2012; data updated September 2018, unpublished).

Table 5.5. Data Requests Submitted to the Bundeszentralregister, 2001–2017

Data Request	Number	Percent
Total applications received	211	100%
Data provided	153	72.5%
Request open (not decided)	4	1.9%
Data not provided	54	25.6%
Application withdrawn or abandoned	26	12.3%
Application rejected	25	11.8%
Applicant directed to a different source	3	1.4%

SOURCE: Götting (2012); data updated September 2018, unpublished.

The analysis of BZR data requests for scientific purposes received from 2000 to 2017 also sheds light on the breadth of institutions working with German criminal-history data (Götting, 2012; data updated September 2018, unpublished).[117] The majority of applications for data (62.1 percent) were submitted by universities and technical colleges. Of these, nearly 85 percent were related to psychology, psychiatry, or criminology. Nearly a quarter (24.2 percent) of applications for BZR data were submitted by public authorities, including the Federal Ministry of Justice, the Interior Ministry, prosecutors, and prisons. The remainder (13.7 percent) were submitted primarily by research institutes. The stated purpose behind the majority of applications was a research project (91.0 percent), followed by a dissertation or a doctoral thesis (4.3 percent) and a legislative proposal (2.4 percent) (Götting, 2012; data updated September 2018,

[116] The count includes four instances in which the reason for the request was a legislative proposal.

[117] In accordance with §42 BZRG.

unpublished). Typically, there are no costs associated with accessing BZR data, although fees may be charged if the application results in considerable work for the BfJ. The waiting time is dependent on the project in question and the amount of labor required in processing the data application. Typical waiting times are about six weeks, although longer waits may occur, particularly if there is a need to clarify various aspects of the proposal.

DEU 4.2 Possibilities and Limitations of the Use of Bundeszentralregister Data for Research Purposes

The use of Central Register data for policy and research purposes is subject to the same limitations as outlined in Section DEU 3.2. In particular, the deletion of entries from the register (in accordance with data retention rules) may result in limited data availability.

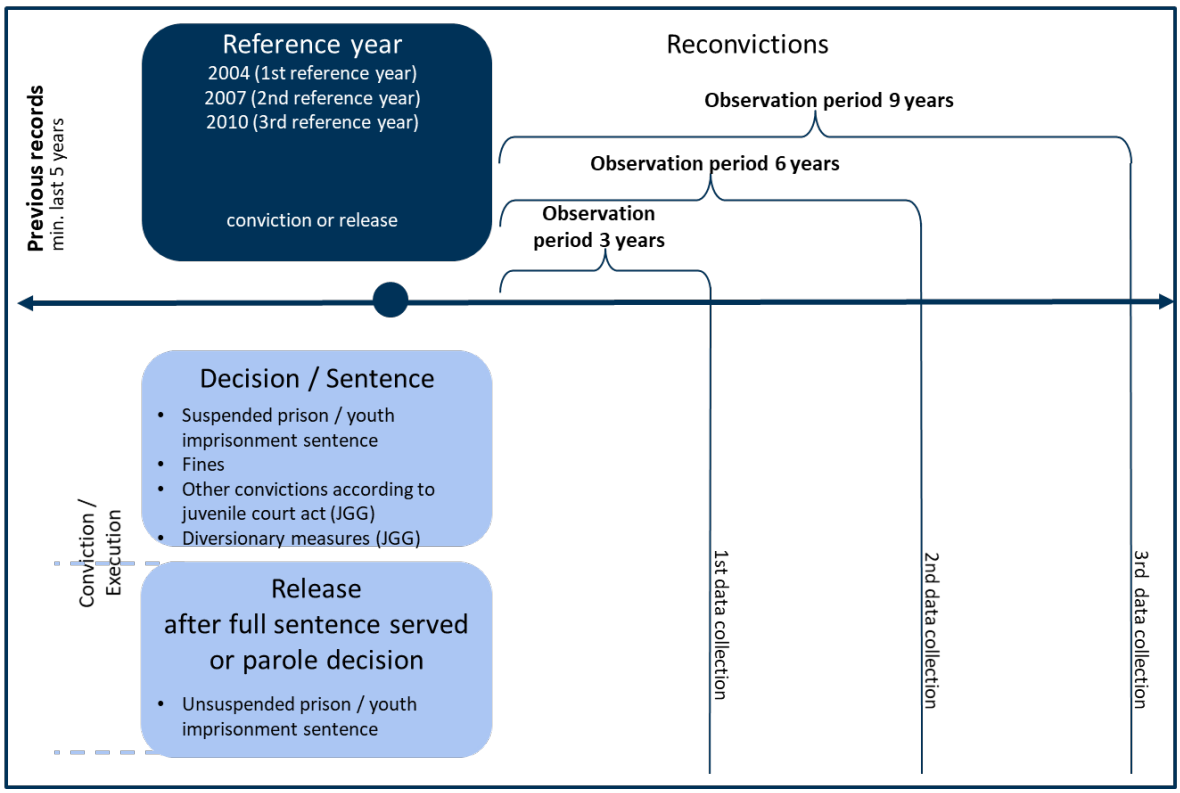
However, German researchers have found a way to overcome the deletion and follow individuals during a longer period if their records have been formally deleted in the BZR. Under the same conditions as discussed in Section DEU 4.1, person-related data from the register can be transmitted two or more times if the public interest warrants it. As specified under §42a Sec. 1a BZRG, data should be pseudonymized.[118] If the individuals from further data collection waves can be individually attached to those of the first data collection, their criminal history can be followed during a longer period even if the original entries have been deleted from the register.

This regulation was the basis of the design used in a nationwide reconviction study commissioned by the Federal Ministry of Justice, which examined the reconviction rate by type of offense, sentence, previous convictions, age, sex, and nationality.[119] The study, organized in three waves, followed all individuals sentenced to a noncustodial measure, fine, suspended prison sentence, or educative measure and all persons released from prison or a posttrial detention during a period of three, six, and nine years (2004 to 2013). In the absence of a national identification number or biometric data, the researchers established an artificial personal key populated by such available information as the date and place of birth, which was pseudonymized using a hash function. The design of the study is shown in Figure 5.2.

[118] See Tolzmann (2015, p. 265) and Bundesministeriums der Justiz und für Verbraucherschutz (2017b).

[119] See Jehle et al. (2016).

Figure 5.2. Research Design of a German National Reconviction Study by Jehle et al. (2016)



To illustrate how BZR data were used, the study determined reconviction and return rates by the type of original sentence after observation periods of three, six, and nine years. The study found that the reconviction rate of released prisoners was about 50 percent after three years and about 63 percent after nine years. However, the return rate (i.e., reconviction to an unsuspended prison sentence) of released prisoners was lower: 25 percent after three years and 34 percent after nine years. Reconviction rates of individuals receiving suspended prison sentences and fines were generally lower. However, the reconviction rates following juvenile justice responses were higher, especially after serving unsuspended juvenile prison sentences: 70 percent after three years and 83 percent after nine years. The return rate for this group was 40 percent after three years and 52 percent after nine years.

6. The Netherlands

Key Findings

- The Judicial Documentation System (Justitieel Documentatiesysteem [JDS]) is the main national-level criminal-history record system in the Netherlands. It includes only data from the prosecution stage and onward, and police data are not included.
- Police data are captured in local and national police recording systems, which are separate from the JDS, and can be accessed through a central national database (Basisvoorziening Informatie [BVI]).

Findings on the Judicial Documentation System

- The JDS is managed by the Judicial Information Service (JustID), an agency of the Ministry of Justice and Security.
- JDS data are primarily provided by prosecution services and courts, although other agencies (e.g., a national correctional agency or child protection board) are also among the reporting entities.
- The JDS is used for operational and civilian purposes. Authorized user agencies have multiple options to query the system (e.g., through an online interface or electronic XML messaging). Civilians typically request an extraction from the JDS via a certificate of conduct.
- A pseudonymized copy of JDS, the Research and Policy Database for Judicial Documentation (Onderzoek- en Beleidsdatabase Justitiële Documentatie [OBJD]), is used for research purposes and is managed by the Research and Documentation Centre, an independent research organization under the aegis of the Ministry of Justice and Security (Wetenschappelijk Onderzoek- en Documentatiecentrum [WODC]).
- The primary objective of the OBJD is to inform the Recidivism Monitor, a long-term research project by the Ministry of Justice and Security that monitors recidivism rates of different groups of offenders over time and evaluates interventions.
- Researchers external to the government can also ask for permission to use data from the OBJD, for example, to test the validity of risk assessment instruments.
- JustID and the WODC (the owners of the JDS and the OBJD, respectively) investigate and correct possible registration errors in the two databases.
- As the owner of the OBJD, the WODC is in the process of preparing to receive and store all identifiable data on individuals. The OBJD may need to acquire this capability to avoid data loss because JustID may be legally required to delete all data on cases after the expiration of their retention period (which is currently used to inform the OBJD).

Findings on Police Databases

- Most of the information captured at the local-level recording system feeds into the BVI.
- Police databases are used for operational purposes but are also accessible for multiple research purposes, including research into criminal careers.
- In general, only the national statistical office receives identifiable data from the police data to enable linkages with other data, such as demographics.
- Everyone registered in the Netherlands has a unique citizen service number (burgerservicenummer [BSN]), and as such, this number is crucial for making data linkages.
- Statistics Netherlands conducts several checks on the data, including plausibility checks, imputation of missing data, and comparing outputs with previous trends to spot possible major outliers.

NLD 1. Overview of the Country and Criminal Justice System

NLD 1.1 The Political and Constitutional System

Since 1848, the Netherlands has been a decentralized unitary state. It currently has 17.3 million inhabitants and consists of one central government, 12 provinces, and 380 municipalities (CBS, 2018a, 2018b; De Graaff-Kamphof, n.d.).[120] In this system, several responsibilities are transferred to the regional and local level, yet these levels of government remain subordinate to the central government (De Graaff-Kamphof, n.d.). These responsibilities include regional economic policy; nature; spatial planning, traffic, and transport at the regional level; and youth care, long-term care, and income support at the local level (De Graaff-Kamphof, n.d.). Criminal justice responsibilities are retained at the level of the central government. However, different organizations are involved in administering the law at the regional and local levels (as further described in Section NLD 1.4).

NLD 1.2 Criminal Code and Procedure

The country operates under a civil (written) law system based on the French civil code, with a limited role for case law (compared to English common law). The Dutch Criminal Code forms the basis of the Dutch criminal justice system and is applicable across the entire country. Similarly, criminal procedures are also similar across the country. Criminal offenses are outlined in the Criminal Code as well as in specific statutes, such as the 1994 Road Traffic Act, the 1928 Narcotic Drug Offenses Act, and the 1991 Military Criminal Code (Tak, 2003). The age of criminal responsibility in the Netherlands starts at 12 years. While children younger than 12 years cannot be prosecuted, they may be subject to civil code measures, such as a juvenile treatment center referral (Tak, 2003). There is no dedicated criminal code for juveniles; the Dutch Criminal Code is also applicable for juveniles of 12 to 18 years of age. However, it includes special provisions for this group, in particular pertaining to trial procedures and sanctions.[121] Under Dutch law, criminal offenses are defined as misdemeanors (*overtredingen*), which include such less serious offenses as driving without a driver's license, and crimes (*misdrijven*), including such more serious offenses as burglary and murder (Van der Leij, 2014).

NLD 1.3 Court Dispositions and Penal Sanctions

Courts, the Public Prosecution Service (Openbaar Ministerie [OM]), and to a limited extent such other bodies as the police can impose sanctions or measures, with courts being the only authority competent to impose custodial measures and prison sentences. Under Dutch law, there are three types of sentences: principal penalties (*hoofdstraffen*), such as custodial sentences;

[120] Population count as of October 2018; municipalities count as of January 2018.

[121] For those aged between 16 and 18 years, the court may decide to convict the offender under the adult criminal justice system (Tak, 2003).

additional penalties (*bijkomende straffen*), such as confiscation of goods; and measures (*maatregelen*), such as disqualification from driving (Van der Leij, 2014). Custodial sentences can be imposed only for crimes, not misdemeanors. Public prosecutors can impose a range of sentences, including (but not limited to) a fine, an alternative sanction of no more than 180 hours of community service, financial compensation for the victim, or an antisocial behavior order (Government of the Netherlands, n.d.f). A similar principle exists for local authorities, police, and other special enforcement officers, who can issue fines for such offenses as antisocial behavior and speeding (Government of the Netherlands, n.d.f). Police can also decide to dispose a case before it enters the prosecution stage and can do so via two main routes: police dismissal (*sepot*) and a criminal decision by the police (*politiestrafbeschikking*) (Van der Leij, 2014). In addition, there is the option to refer juvenile offenders to an alternative punishment program (*Halt*). In the case of a police dismissal, there is no prosecution, and the police will not issue an official police report, although the details of the case may still be used in case of reoffending (Van der Leij, 2014). A politiestrafbeschikking is a form of prosecution in which a sentence is imposed (e.g., a fine).

NLD 1.4 Criminal Justice Agencies

As the leading authority in the Dutch criminal justice system, the Ministry of Justice and Security (Ministerie van Justitie en Veiligheid) is responsible for a variety of organizations and agencies relevant for the administration of the criminal justice system (see Box 2 for examples). This section will focus on key agencies in the criminal justice system based on their involvement in or responsibility for criminal-history record systems in the Netherlands.[122] These agencies are referred to throughout this chapter as they either contribute data to or work with data from the national criminal-history information system.

Box 2. Organizations and Agencies Functioning Under Responsibility of the Dutch Ministry of Justice and Security

- **Central Judicial Collection Agency** (Centraal Justitieel Incassobureau). Responsible for collecting various types of fines, coordinating sentences and arrest warrants, and providing management information to the justice chain.
- **Child Care and Protection Board** (Raad voor de Kinderbescherming). Responsible for protecting the rights and needs of children.
- **Custodial Institutions Agency** (Dienst Justitiële Inrichtingen [DJI]). Responsible for carrying out custodial measures and prison sentences.
- **Judicial Implementation Service Testing, Integrity, and Screening** (Justitiële uitvoeringsdienst Toetsing, Integriteit en Screening [Dienst Justis]). Primarily responsible for preemployment screening.
- **JustID.** Responsible for registration and provision of judicial and criminal data and for facilitating information exchange in the criminal justice chain. Key aim is to provide access to "an honest and integral overview of an individual" (JustID, n.d.a).
- **Judiciary** (Rechtspraak). Operating independently of the Ministry of Justice and Security and consisting of 11 district courts, 4 courts of appeal, and 1 Supreme Court.
- **Netherlands Police** (Nationale Politie). Responsible for law enforcement and emergency assistance.

[122] With the exception of Dienst Justis, the Judicial Information Service, and the Research and Documentation Centre.

- **OM.** Responsible for investigation and prosecution of crimes. Note that "the service functions under responsibility of the Minister of Justice, but it is not an agency of the Ministry of Justice. The service is part of the judiciary" (Tak, 2003, p. 28).
- **WODC.** Responsible for conducting, commissioning, and documenting scientific research for the Ministry of Justice and Security.

SOURCE: Government of the Netherlands (n.d.c).

Law enforcement: Between 1994 and 2013, the Dutch police force consisted of 25 autonomous regional police units and 1 central police force (Korps Landelijke Politiediensten— [Netherlands Police Agency]) (Politie, n.d.a). In order to better respond to new societal challenges, the national Netherlands Police (Nationale Politie) was established in January 2013, led by a police commissioner (*korpschef*) and his team (commissioner's staff) and further consisting of ten regional units,[123] one central unit (Landelijke Eenheid), and a Police Service Centre (Politiedienstencentrum) (Politie, n.d.a). Each regional unit is made up of geographical districts at the local level (43 districts across the Netherlands), which have specialist local departments, such as drug crime investigation teams (Gemeente.nu, 2002; Politie n.d.b). These districts in turn consist of "frontline teams" (*basisteams*), including neighborhood police officers (167 teams across the Netherlands) (Politie n.d.b, 2012). The central unit deals with national as well as international crimes (e.g., cybercrime and terrorism) and security-related issues (e.g., protection of the Dutch royal family) (Politie, n.d.b). The police organization's back office is managed by the Police Service Centre.

Prosecution: OM operates under the political responsibility of the Ministry of Justice and Security and is headed by the board of procurators-general (College van procureurs-generaal) (OM, 2017a). OM has the exclusive right to bring criminal proceedings and can either take cases to court or dispose cases itself (e.g., through a settlement) (Tak, 2003).

While in theory OM bears the ultimate responsibility for criminal investigation, in practice these investigations are mainly conducted by the police (in consultation with the public prosecutor) (Tak, 2003). However, public prosecutors have become more actively involved in criminal investigations through issuing instructions for dealing with specific offenses.[124]

OM consists of ten regional offices (*arrondissementsparketten*), and each is led by a chief public prosecutor (OM, 2017a, 2017b). These regional offices are aligned with the ten regional police units and based in the same city as the regional district court (OM, 2017a, 2017b). Appeal cases are dealt with in one of the four Appeal Court Public Prosecution Offices (Ressortsparket) located in the same cities as the appeal courts (OM, 2017b). The prosecutors at the Supreme

[123] Consisting of the following regional units: Noord-Nederland, Oost-Nederland, Midden-Nederland, Amsterdam, Den Haag, Rotterdam, Zeeland West-Brabant, Oost-Brabant, and Limburg (Politie, n.d.c).

[124] According to Tak (2003), "This may be a result of the increasing complexity of cases and the lack of financial resources, which has made it necessary to fix priorities when instituting investigations. Furthermore, the Supreme Court's rulings on inadmissible evidence have increasingly stressed the importance of public prosecutors in ascertaining, as early as possible, what methods should be employed in the investigation" (p. 28).

Court operate independently of OM (Tak, 2003).[125] In addition to the regional offices, OM has three national offices.[126]

Courts: Criminal cases are dealt with by districts courts (*rechtbanken*), courts of appeal (*gerechtshof*), or the Supreme Court (Hoge Raad). There are 11 district courts, 4 courts of appeal, and 1 Supreme Court (Rechtspraak, 2017). Depending on the severity of the offense, cases in district and appeal courts are dealt with by a single judge or a full bench of three judges (Tak, 2003). District courts could act in different capacities, such as a cantonal court (*kantongerecht*, dealing with misdemeanors only), a police court, an economic police court, and a juvenile court (Tak, 2003).

While district courts and courts of appeal deal with the facts of cases brought forward, the full bench of judges (five) at the Supreme Court review "the lawfulness of judgments of lower courts and the manner of proceedings" (Tak, 2003, p. 33).

Corrections: The DJI, part of the Ministry of Justice and Security, is responsible for carrying out custodial measures and prison sentences (DJI, n.d.b, 2017). The DJI operates at 50 locations across the Netherlands, comprising various types of facilities, such as remand centers, adult prisons, juvenile detention centers, and psychiatric centers (DJI, 2018).[127]

Across these different institutions and centers, approximately 36,000 new detainees are admitted annually (DJI, 2019). According to the latest figures from the DJI, on average, adult and juvenile offenders are detained for 110 days and 3 months, respectively (DJI, 2019). Based on 2017 data, a majority (52 percent) of adults remained in prison for less than a month, 39 percent were detained between 1 and 12 months, a small proportion (7 percent) were detained for over 1 year, and 34 adults were serving life sentences in 2016 (DJI, 2019). Patients spend on average 7.5 years in forensic psychiatric centers (DJI, 2019). Foreign nationals are held in detention centers on average for 6 weeks (DJI, 2019).

Probation services are funded by the Ministry of Justice and Security and are provided by three organizations (3RO): the Dutch Probation Service (Reclassering Nederland, responsible for roughly 60 percent of the cases), the Dutch Addiction Probation Service (Stichting Verslavingsreclassering GGZ, responsible for roughly 30 percent of the cases), and the Salvation Army Youth Care and Probation Service (Stichting Leger des Heils Jeugdbescherming en Reclassering, responsible for roughly 10 percent of the cases) (DJI, n.d.a).

---

[125] "The prosecution office attached to the Supreme Court is not part of the prosecution service. It forms an independent office with special tasks and powers" (Tak, 2003, p. 31).

[126] This includes the National Public Prosecutor's Office (Landelijke Parket), which deals with (inter)national organized crime; the National Public Prosecutor's Office, for serious fraud and environmental crime and asset confiscation (Functioneel Parket); and the Central Processing Unit (Parket Centrale Verwerking OM), which deals with such cases as appeals for minor traffic violations, drunk driving, and driving without insurance (OM, 2017a, 2017b).

[127] Since 2010, the DJI is also responsible for carrying out custodial measures and prison sentences in the Caribbean Netherlands (Bonaire, St. Eustatius, and Saba) (DJI, 2019).

NLD 1.5 Size of Criminal Justice System

In 2017, there were approximately 831,000 police-recorded crimes in the Netherlands, corresponding to a rate of 49 per 1,000 population.[128] The majority (61 percent) of recorded crimes were property offenses, and violent and sexual offenses represented 17 percent of the total. Nearly 225,000 crimes (27 percent of the total) were cleared by the police, and a total of approximately 245,000 suspects were identified for these cases (ca. 170,000 unique persons). Among unique individuals identified as suspects, approximately 18,500 (11 percent) were minors (Smit and Kessels, 2018).

Public prosecutors processed about 183,000 cases in 2017. A slight majority (53 percent) of these cases proceeded to court, 18 percent were unconditionally dismissed, and 17 percent were resolved with a penalty order (*strafbeschikking*). Most of the remaining cases were either conditionally dismissed or resulted in a fine, a compensation order, or community service (Decae and Netten, 2018).[129]

First instance courts in the Netherlands adjudicated approximately 93,000 cases in 2017. In the vast majority (89 percent) of cases, the defendant was found guilty; 10 percent of cases resulted in acquittals. Slightly fewer than half (45 percent) of all guilty verdicts were followed by a prison sentence or juvenile detention. Of these, in approximately 30 percent of cases, the prison sentence or juvenile detention was combined with either community service or a fine or both. In 2017, the majority (53 percent) of prison sentences were less than one month long.[130] A quarter (25 percent) of all guilty verdicts resulted in a fine only, and a similar proportion (27 percent) was punished by community service only (Vink and Van den Braak, 2018).

The prison population in the Netherlands stood at 35,250 in 2016 (CBS, 2017),[131] corresponding to an incarceration rate of 53 per 100,000 population (Aebi, Tiago, and Burkhardt, 2017).[132]

NLD 2. Judicial Documentation System

This section provides an overview of the key national criminal-history record system in the Netherlands—the JDS. In addition to the JDS, information on individuals who come into contact

---

[128] Based on provisional figures. Offenses recorded by the police include offenses as laid down in the Criminal Code, the Narcotic Drug Offenses Act, the Arms and Munitions Act, and the Road Traffic Act.

[129] A conditional dismissal (*voorwaardelijk beleidssepot*) does not mean that a condition has been imposed on the suspect. It means there are case-specific conditions due to which the prosecutor can decide there is no public interest in prosecution. Examples of these conditions include if the offense took place a long time ago, if the offense was relatively insignificant, if the suspect is of poor health or has been recently punished, or if there are reasons connected to the relationship between the suspect and the victim.

[130] Excluding juvenile detention.

[131] Detainees include those who were convicted, as well as those placed in temporary custody (CBS, 2017).

[132] Prison rates are calculated based on the situation of penal institutions on September 1, 2005, and September 1, 2015 (Aebi, Tiago, and Burkhardt, 2017).

with the criminal justice system is also captured in local and national police recording systems. These police databases are described in NLD Appendix A.

NLD 2.1 History and Organizational Management

The JDS is maintained and operated by JustID of the Ministry of Justice and Security. The criminal records obtained from the JDS are called *uittreksel justitiële documentatie*.

The legal basis for the JDS is provided by two legal instruments (JustID, 2009):

- **Dutch Code Concerning Data Used in Judicial Settings and Criminal Proceedings** (Wet justitiële en strafvorderlijke gegevens). Outlines rules regarding what information should be registered, the period during which information should be registered, and access arrangements (for whom, for what purpose, and type of information for which access is granted).
- **Judicial Data Act** (Besluit justitiële gegevens). Establishes the type of offenses that should be registered as well as the details on when public authorities are permitted access to the JDS.

While the JDS is primarily used for operational purposes, a pseudonymized copy of this database, the OBJD, is used for research purposes. Section NLD 4 focuses on the OBJD in more detail.

NLD 2.2 Content

Since 1996, the JDS has provided a centrally organized overview "of all natural and legal persons that have come into contact with the judicial system in the Netherlands [i.e., from case registration at the public prosecutor's office onward], and of cases they were suspected of" (Wartna, Blom, and Tollenaar, 2011, p. 9). The JDS also stores information on acquittals, dismissals, and cases that are not dealt with by courts yet. There are no specific procedures for juveniles; criminal records are kept for all suspected or convicted individuals of the age of criminal responsibility (12 years and older). In addition, the JDS stores information on foreign judgment against Dutch citizens. As of September 2017, the system held data on approximately 2.75 million persons, of which 110,000 were legal entities (e.g., companies) (JustID, 2017b). Police data are not captured in the JDS. (These are captured in the local and national police databases, which are described in NLD Appendix A.)

In the years leading up to the centralization and automation process of the JDS, judicial data were first captured on hard copy cards at each local public prosecutor's office, after which they were sent to JustID's predecessor (the Central Judicial Documentation Office), which then stored the data as images (Wartna, Blom, and Tollenaar, 2011). Since 1996, these data from public prosecutors' offices and district courts feed directly into the JDS.[133] As such, the JDS has data on

[133] For example, via the OM system called Integrated Process System Criminal Law (Geïntegreerd Processysteem Strafrecht [GPS]).

all individuals who have been in contact with the judicial system in the Netherlands since 1996. For some individuals, this includes information from the images as stored pre-1996: "When the JustID receives notification of a new criminal case involving an individual, it also examines whether this person was involved in any cases that were stored as an image. If that is the case, these old cases are entered into the JDS" (Wartna, Blom, and Tollenaar, 2011, pp. 9–10). This process of entering images as stored pre-1996 into the JDS is also applied for individuals who do not appear in the JDS yet but have been subject to investigations during or after 1996.

With respect to offense types, the JDS captures all crimes and misdemeanors that are reported to police and referred to prosecutors (JustID, 2009). Examples of misdemeanors captured in the JDS include those punishable by a fine of €100 or more and those punishable by imprisonment. Minor traffic offenses are excluded from the JDS.[134] Criminal matters that cannot be pursued due to the statute of limitations (*verjaarde zaken*), including cases predating 1996, are also not included (Overheid.nl, 2016; Wartna, Blom, and Tollenaar, 2011).

Information collected in the JDS includes

- name, place and date of birth, unique BSN, address, and citizenship
- data on the offense in question[135]
- data on the outcome of the case (sentence details and deciding authority, e.g., juvenile/adult or cantonal court)
- location of the offense and reporting agency (JustID, 2017b; Wartna, Blom, and Tollenaar, 2011).

The JDS does not record biometric data due to legal limitations. Biometric data (fingerprints and photos), collected when a person is taken into custody, are held in a separate database maintained by JustID called the Criminal Justice Chain Database (Strafrechtsketendatabank [SKDB]). This database holds individuals' personal information for identification purposes.[136] DNA information is held in a separate database managed by the Dutch Forensic Institute.[137]

The JDS also maintains the Personal Document System (Persoonsdossier Systeem [PDS]), which collects all psychiatric and psychological reports that have been presented to the judiciary by the Child Care and Protection Board and probation services over the past ten years (JustID, n.d.d). JustID is currently transferring the hard copy reports of the PDS to a digitalized system (JustID, n.d.d). The PDS may include reports on individuals (mostly youths) who do not have a

[134] This covers traffic offenses that fall under the Act on Administrative Enforcement of Traffic Regulations (Wet administratieve handhaving verkeersvoorschriften, or Wet Mulder).

[135] Date of arrest is not available in the JDS.

[136] The database includes the following information: biographic information, residency information, address (as recorded by municipalities), detention facility address (if applicable), and last known address. An example of a personal file can be found at JustID (2011). The Strafrechtsketennummer, a number assigned to individuals in the SKDB data bank, can, in conjunction with a surname, be used to search the JDS (see Section NLD 2.4).

[137] More information can be accessed at Nederlands Forensisch Instituut (n.d.).

criminal record on the JDS. The existence of a PDS record is not contingent on whether a person has been prosecuted.

The primary contributors of data to the JDS are public prosecutors' offices and the courts; however, other agencies (e.g., the child protection board or EU partners) contribute content to the JDS. There are three ways in which data are provided to the JDS: electronically, manually (by post), or through an upload via JDS's online application, JD-Online. Criminal record information is mostly provided electronically, and very few criminal records are uploaded manually. JD-Online is used exclusively to input information into the PDS. Contributing agencies do not have the right to edit entries directly on the JDS; submitted data are checked by JustID and subsequently stored on the system. The same process applies to subsequent modifications and amendments; they are done by JustID based on received information. The system receives approximately 700,000 information submissions every year (JustID, 2017b).

NLD 2.3 Data Retention

Retention rules pertaining to records in the JDS differ based on offense type and depend on the legal storage term for these offenses (JustID, 2009; Wartna, Blom, and Tollenaar, 2011). In general, record retention periods are longer for more serious crimes that include imprisonment than for misdemeanors (JustID, n.d.e). Table 6.1 shows the retention periods for criminal offenses.

If the individual dies during the legal storage term, the record retention period is subject to limitations on how long information can be stored after the person's death. Data are either deleted at the end of the original retention period or at the end of the post-death retention period, whichever comes first. For misdemeanors, data cannot be retained longer than 2 years after death. For crimes where the highest possible prison sentence (according to the legal description) is shorter than 6 years, this period is 12 years after death (Overheid.nl, 2016). In cases where a sentence of 6 years or more can be imposed, the data can be retained for 20 years after death.

Table 6.1. Judicial Documentation System Retention Period by Type of Offense

Retention Period	Type of Offense
5 years	Sentences for misdemeanors
10 years	Sentences imposed for misdemeanors that hold a custodial sentence, excluding civil imprisonment, a community service order, or the imposition of a fine of the third category (€4,101–€8,200)[a] or higher
20 years	Sentences for crimes for which the maximum sentence is less than 6 years imprisonment
30 years	Sentences for crimes for which the maximum sentence is 6 years imprisonment or more
50 years	Custodial sentences or measures involving deprivation of liberty for more than 20 years
80 years	Life imprisonment or measures involving deprivation of liberty for more than 40 years Sentences for sexual offenses

SOURCE: Overheid.nl (2016, Art. 4).
[a] Government of the Netherlands (n.d.a).

The record retention lengths are the same irrespective of how the underlying case was resolved and apply equally to people with and without convictions (Overheid.nl, 2016). Individual cases may differ, however, with respect to when the legal storage term commences. The possibilities are

- when the public prosecutor takes the decision not to prosecute (where a case is dropped)
- when a penalty order (*strafbeschikking*) imposed by the public prosecutor has been fully executed (for cases where the prosecutor decides to impose one)
- when a definite verdict is passed by a court (for cases that go to court) (JustID, n.d.e).

In the event an individual receives a new conviction while the retention period is in effect for an already existing record, the record will be retained until the expiration of all applicable retention periods (JustID, n.d.e). Thus, if people have multiple records, no record will be deleted until all records are eligible for deletion.

In practice, when the retention period of a given record has elapsed, the information is not deleted from the JDS. Instead, JustID automatically applies a filter, which renders the record invisible to any searches for operational and civilian purposes. In strictly technical terms, it would be possible to reinstate expired records and make them visible again; however, there are no legal grounds for doing so except to make the data available for research purposes. In the near future (a decision is pending at the time of the writing of this report), there may be a change in how expired cases are handled, and JustID may be required to delete all expired cases. As discussed in Section NLD 4.4, this change would have implications for the OBJD research database, which currently receives linked identifiable data from the JDS.

Dutch law also recognizes the possibility of a convicted individual being granted a pardon (*gratie*) from the government based on a recommendation by a court. A pardon does not change anything about the underlying convictions but changes the execution of the remainder of the sentence, which may be fully or partially commuted (Boogaard and Uzman, 2019). When a pardon is granted, pertinent information (date and number of the decree and attached provisions) is recorded, and no other changes to criminal data are made.

NLD 2.4 Access to and Use of the Judicial Documentation System for Operational and Civilian Purposes

Institutional Access for Operational Purposes

The JDS has numerous users. Entities that are authorized to access JDS information and query the system for operational purposes include the police and the JDS's contributing criminal justice agencies. In addition, other public authorities, such as local authorities, may be granted access to JDS data under specific regulations as established in the Judicial Data Act. The Judicial Data Act specifies "information objectives" (*informatiedoelstellingen*) under which JDS data may be accessed: provision of certain information, provision of general information, and provision of information to other countries.

Table 6.2 provides an overview of these three information objectives, along with a description of operational purposes corresponding to these objectives and what type of information is available under each objective. However, please note that this overview is a high-level simplification of the applicable rules. Specific, granular conditions of data access by individual organizations (including type of data, purpose of data access, preconditions of access, data retention, and sharing with third parties) are frequently addressed by secondary legislation referred to in the Judicial Data Act. NLD Appendix B contains a nonexhaustive illustration of organizations that have access to JDS data mapped against each information objective listed above.[138]

Table 6.2. Access to Judicial Documentation System Data for Operational Purposes

Information Objective	Corresponding Operational Purposes	Type of JDS Data That Can Be Typically Provided
Provision of certain information	Execution of an agency task	Convictions resulting in an unconditional sentence, typically no later than 4 years after the end of sentence execution
	Provision of advice	
	Administrative decision by the agency	
Provision of general information	Execution of an agency task	All JDS information
	Recruitment or dismissal of staff members	
	Provision of advice, recommendation or nomination of persons	
Provision of information to third countries	Third-country agency operations	All JDS information

Information from the JDS can be accessed multiple ways. Authorized users external to JustID can query the system via the online interface JD-Online, through a messaging application, or via electronic message traffic (e.g., XML). Some users (e.g., municipalities) are provided information in hard copy, although hard copies are being phased out (JustID, 2017b).

There are four ways in which the JDS can be queried (depending on what information is available to the requestor): using personal information (first name(s), surname, and place, country, and date of birth); a docket number and a surname; BSN and a surname; and Strafrechtsketennummer (the number assigned to individuals in the SKDB data bank) and a surname. The first type of query can result in multiple hits as the system returns close matches; the remaining three options return either a precise match or no hits.

[138] In addition to these structured reasons for data sharing, the Dutch Code Concerning Data Used in Judicial Settings and Criminal Proceedings also allows for incidental or ad hoc sharing of criminal-history data under special circumstances and for reasons of important public interest (Helsloot et al., 2013).

In 2016, approximately 9 million requests for JDS information were made, of which just over 2 million were conducted by using JD-Online (JustID, 2017b).

Access to and Use of the Judicial Documentation System for Civilian Purposes

Individual Access to Verify Personal Records

Any individual can request to inspect what data are registered in their name in the JDS. This application for civilian purposes is subject to a fee. Once the extract from the JDS is available, individuals must review the data at the district court in the place of their residence (JustID, n.d.c).

Access through Certificate of Conduct

Access to the JDS for civilian purposes is also possible via a certificate of conduct (*verklaring omtrent gedrag* [VOG]), used to prove that a person's behavior in the past cannot be an obstacle to fulfilling a specific role in an organization or a society (Justis, n.d.g). The certificates are issued (or declined to be issued) based on the results of background checks conducted by the Dienst Justis. For some professions, it is a legal obligation to obtain a VOG; in other cases, it is up to the employer to make the submission of a VOG a requirement for a certain position (Justis, n.d.f). The employer also decides on which aspects an individual will be screened, depending on the nature of the role (Justis, n.d.e). The request can be submitted either online or in hard copy to one's municipal authority.[139]

On receiving the application, Justis establishes whether a person has a criminal record. To conduct these checks, Justis uses different databases: the JDS, police databases, and specific information from OM or Probation Services. If nothing is found, the person in question automatically obtains a VOG (Justis, n.d.a). In situations where it emerges that there is a criminal record, Justis first determines whether there have been any criminal offenses relevant to the purposes of the application over the period under review (usually four years, but there are several exceptions depending on the purpose of the request and the age of the applicant) (Justis, n.d.c). Subsequently, the decision whether to issue a VOG with a criminal record is determined by both objective and subjective criteria (Staatscourant, 2017). The objective criterion considers the nature of the criminal record and assesses the risks to society should there be a recurrence of criminal activity. It also assesses whether the recurrence would constitute an obstacle to a proper execution of the job or activity for which the VOG is being sought. Even when no relevant offenses are discovered, Justis might still decide to refuse the application based on a red line of irrelevant offenses that creates a negative impression of the applicant's integrity and, therefore,

[139] The application can also be made directly to Justis if the person is not registered in the Personal Records Database (Basisregistratie Personen), which includes details on individuals living in the Netherlands and Dutch citizens living abroad. Every person registered in the database automatically receives a BSN (Government of the Netherlands, n.d.b, n.d.e).

reason to believe there is a credible danger to society.[140] The subjective criterion subsequently assesses whether the interest of the applicant in receiving the VOG outweighs the risk to society. If that is the case, the VOG will be issued even if the objective criterion for refusing the issuance is met. This is because the refusal to issue the VOG would be considered as disproportionately affecting the individual.

The risk to society is expressed in eight distinct risk categories pertaining to the following domains: information, money, goods, services, business transactions, process, management, and persons (Staatscourant, 2017). The applicant is required to indicate whether his or her job would feature responsibilities related to these eight domains. In addition, the screening is undertaken either against a general applicant profile or against 1 of 16 predetermined screening profiles developed for specific employment sectors and application purposes.[141] These targeted profiles specify the potential risks in greater detail and help determine whether the applicant's criminal-history information is relevant for the purposes of the VOG application.

If issued, the VOG describes which screening profiles have been applied and what risk assessments have been undertaken. As stated above, even when a certain crime is outside the scope of a specific profile, it can still be the reason for the refusal of issuing the VOG (Justis, 2018). Justis makes a decision within four to eight weeks of receipt of the application (Justis, n.d.b). If an application is successful, Justis sends the VOG (exclusively) by mail to the employee directly, not to the employer (Justis, n.d.d).

NLD 3. Addressing Judicial Documentation System Data Quality and Completeness

JustID regularly investigates and corrects possible registration errors in the JDS, such as situations where data pertaining to one individual may be attached to the name of multiple "seemingly different individuals" (Wartna, Blom, and Tollenaar, 2011, p. 10). Individuals have an option to apply for a review of their own records and have an opportunity to subsequently initiate a correction (JustID, n.d.c). If a person believes their data are wrongly recorded or incorrect, they can submit a correction or deletion request to JustID (either by email or in writing). This request should contain the desired changes. A written decision by the Minister of

[140] The objective criterion may also be met if a person has only irrelevant criminal records registered during the review period and at the same time there is also at least one relevant offense registered outside the review period (Staatscourant, 2017). A report on the effectiveness of the VOG commissioned by the WODC found that the red line criterion may have been at times interpreted too widely, to the detriment of the applicant (Kruize and Gruter, 2016).

[141] The 16 profiles are political office holders; visa and emigration; housing permit; (special) enforcement officer; holiday host family and adoption; health care and welfare of humans or animals; operating license for a catering establishment; legal services; education; taxi industry (taxi drivers permit); taxi industry (operator's license); family supervisor, probation officer, child welfare investigator, and social worker; sworn interpreters/translators; membership in a shooting club; financial services; and unknown employment (Justis, 2017).

Justice and Security is made in response to the request within four weeks. If the applicant is not satisfied with the decision, a written objection can be submitted within six weeks. In a case where it has been decided to correct the data, all persons and organizations that have received data of the person in question over the past year need to be informed of the correction as soon as possible (Overheid.nl, 2016).

In 2016, JustID launched a project called Focus on Data Quality, intended to improve the quality of data held in the JDS. In response to observed errors in data as well as in message traffic, the project primarily focuses on data collection and registration from reporting agencies and the transmission process to the JDS (JustID, 2017a).[142] Correspondingly, the project is organized in two stages. The first focuses on monitoring and potential improvements in messaging traffic. The second involves a comparison of JDS data with source files held by public prosecutors and the courts over the last ten years. The comparison is undertaken utilizing big-data analytical approaches, and the Netherlands Forensic Institute provides assistance to the project by making its expertise available to support the file comparison. Based on the results of this analysis, JustID and its partner agencies will produce plans to reconcile any differences. Simultaneously, JustID has also established a dedicated virtual Data Quality Office with the participation of representatives from JustID, OM, and the Central Judicial Collection Agency.

Specifically with respect to the OBJD, the WODC conducts several checks to address (and avoid) deficiencies. Every time new data are added to the database and the system is refreshed, a check is performed to verify whether any unanticipated changes may have taken place. If a discrepancy is found, the WODC will manually investigate the case in greater detail. Verifications are also performed with respect to data counts and set preconditions, such as checks on duplicate cases, and on whether cases on appeal are referred to by the correct appeal case number. In addition, on the receipt of the new data, the WODC adds details that facilitate research, such as classifying offenses and listing the different sentences for a particular offense, since the JDS provides only the article of the Criminal Code. This process takes about one week. Lastly, the WODC gleans additional insights into the quality of data by retrospectively recalculating the reconviction rates for all cohorts and comparing those with previous results (Wartna, Blom, and Tollenaar, 2011, p. 10).

[142] The need to focus on data registration was also highlighted by an interviewee, who commented that the Council for the Judiciary (Raad voor de Rechtspraak) conducted a separate, small-scale internal study into registration errors and found that not all relevant fields included in the data set were completed by the court administrators.

NLD 4. How Are Criminal-History Record Data used for Research Purposes?

NLD 4.1 Technical Details of the Research and Policy Database for Judicial Documentation

As mentioned in Section NLD 2, the OBJD, a copy of the JDS, is available for research purposes. The main reason for creating the OBJD in 2001 was to be able to measure and study recidivism, including recidivism trends, in a structured way. Correspondingly, the Recidivism Monitor research project (discussed in Section NLD 4.3) is one of the main outputs based on the OBJD.[143]

The Ministry of Justice and Security is the holder of the OBJD. The research component and user application of the OBJD is maintained and operated by the WODC, an independent research organization under the aegis of the Dutch Ministry of Justice and Security. The technical component of the database is owned by JustID. The OBJD is a pseudonymized version of the JDS, in which names are not included and other identifying data are encrypted for privacy reasons (Wartna, Blom, and Tollenaar, 2011). The OBJD includes a copy of relevant tables as included in the JDS, including information on the offenses, offenders, and case outcomes.

JDS data for the OBJD are provided by JustID on a quarterly basis and used biannually to inform the Recidivism Monitor project. Data are received utilizing a strict, automated procedure via a secure file-transfer protocol connection, after which they are encrypted and imported into the OBJD. Data in the OBJD are stored indefinitely and remain available even after the legal storage term of the corresponding data in the JDS has expired. As of January 2018, the OBJD contained data on almost 4.5 million individuals and about 14 million criminal cases.

NLD 4.2 Procedures to Access the Research and Policy Database for Judicial Documentation Data for Research Purposes

Researchers at the WODC are permitted to use the OBJD for research purposes. External researchers can also request permission to use data from the OBJD. To access the data, researchers must submit a formal request to the WODC, detailing their research proposal. The WODC assesses the scientific merit of the proposal by looking at the logical structure, transparency, and replicability. If granted permission, researchers receive anonymous data via a

[143] In 2011, the WODC published an English version of the *Memorandum of the Recidivism Monitor* (Wartna, Blom, and Tollenaar, 2011). The memorandum provides a detailed account of the OBJD, its content, and its use for the Recidivism Monitor. Given the comprehensive nature of the document, this section draws substantially on this memorandum. Where available, additional details as obtained through interviews are included.

secure transmission line. The WODC asks for financial compensation for the processing of applications.[144] The processing time of a data request takes about three months.[145]

In 2015 and 2016, permission to use the OBJD was granted to 15 researchers. The goals of their studies included testing the validity of risk assessment instruments, examining criminal careers, and conducting effect studies.

NLD 4.3 Use of the Research and Policy Database for Judicial Documentation for Research Purposes

The main research output of the OBJD is the Recidivism Monitor research project of the WODC. The Recidivism Monitor "is a long-term research project that conducts standardized measurements of recidivism amongst diverse groups of offenders" (Wartna, Blom, and Tollenaar, 2011, p. 7).[146] Two main purposes of the Recidivism Monitor are to monitor recidivism rates of various groups of offenders over time and to study the effects of penal interventions:

- **Monitoring of specific offender groups.** Adult and juvenile offenders subject to criminal proceedings, former prisoners, former juvenile inmates, and former patients of forensic psychiatric centers are monitored through biannual measurements. To interpret trends in recidivism, the descriptive rates are adjusted by controlling for different characteristics that correlate with recidivism (e.g., gender, number of previous offenses, and age of onset). The unadjusted recidivism rates on different offender groups are available through the REPRIS application on the WODC website (Wartna, Blom, and Tollenaar, 2011).[147]
- **Program and policy evaluation.** The OBJD is also used by the WODC for studying the effects of different interventions aimed at preventing recidivism. Examples of recently conducted effect studies are the Institution for Persistent Offenders (Inrichting voor Stelselmatige Daders) measure, the Social Conduct Order (Gedragsbeïnvloedende Maatregel), and cognitive skills training.

NLD 4.4 Data Linkage and Future Arrangements

Data sharing between JustID (which maintains the JDS) and the WODC (which maintains the OBJD) is currently arranged under a letter of agreement. Historically, JustID had sole

---

[144] A request for the criminal history of 100 persons costs €1,525; a request for the criminal history of 1,000 persons costs €1,750; and a data request of for the criminal history of 10,000 persons costs €4,000.

[145] According to unpublished information shared by the WODC.

[146] Minor offenses (unless the study aim requires a focus on specific offenses, such as traffic offenses), as well as acquittals, court clearances of charges, and "dismissal by reason of unlikelihood of conviction" are not included in the monitor. Cases that are pending or on appeal are included (Wartna, Blom, and Tollenaar, 2011, pp. 13–14).

[147] "REPRIS shows the raw data, not corrected for changes in the composition of the research population. They show the level of recidivism, but show no causes or effects. They are solely descriptive statistics not reducible to individual persons. For technical and privacy reasons, statistics are not shown when the research group is smaller than 15 or when the reconviction rates are higher than 90%" (Wartna, Blom, and Tollenaar, 2011, p. 21).

responsibility for linkage of identifiable data included in the JDS, as the WODC received only an anonymized version of the JDS. At the time of the writing of this report, a decision is pending on whether JustID will be legally required to delete all data on expired cases (i.e., cases that are no longer visible via searches of the JDS). In the event of such a decision, which would impede the data linkage process, the WODC would receive and store all identifiable data on individuals in the future, to avoid loss of criminal career data. Until that point, JustID would still link identifiable data when requested, while the WODC conducts linkage with encrypted data.

7. Comparative Chapter

The country chapters included in this report demonstrate how individual countries organize and manage their national criminal-history information systems. This chapter provides a comparison across all the countries, with the aim of identifying common themes as well as highlighting notable points of divergence. The chapter first provides a brief overview of selected statistics on the countries' criminal justice systems, followed by a discussion of similarities and differences in the countries' national criminal-history information systems. This discussion focuses on the following aspects: characteristics of the criminal record information system, content of the system, access to the system, and data quality and completeness.

Characteristics of National Criminal Record Information Systems

There are discernible differences across the countries in the functions that their national CRIS are designed to perform (see Table 7.1). Two broad organizational approaches can be distinguished. In Australia, Canada, England and Wales, and the U.S., the national systems are maintained by specialized departments of law enforcement or criminal justice agencies and are designed to capture information on the history of an individual's interaction with the criminal justice system. In these countries, data typically start being collected at the moment of arrest or when a person is charged by the police with an offense.[148] The national CRIS in each of these countries also contains or is linked to databases containing noncriminal-history information, such as a database of missing persons. For example, the Canadian National Repository of Criminal Records is one of four data banks included in CPIC, not all of which include criminal information.

By contrast, in the Netherlands and Germany, the national system is maintained by specialized governmental agencies falling under the responsibility of the national Ministry of Justice. In Germany, the responsible agency is the Federal Office of Justice, an agency of the Federal Ministry of Justice, which functions as a service authority of the German judiciary (BfJ, n.d.b). In the Netherlands, the national CRIS is maintained by JustID, an agency of the Dutch Ministry of Justice and Security. In these countries, data collection for the national CRIS starts later as individuals progress in the criminal justice system and is not initiated by police agencies. For their records to appear in the national system, individuals in the Netherlands must be prosecuted for the alleged offense, while individuals in Germany must be convicted.[149]

[148] However, there is some variation across jurisdictions in Australia.

[149] Public prosecutor and court disposals of juvenile cases (with or without the imposition of a conditional measure) are also recorded.

The countries also differ on whether they have a centralized information system for sharing police data (e.g., information on criminal investigations) that is separate from the national CRIS. In Germany and the Netherlands, law enforcement agencies make use of national police databases that exist alongside the national CRIS. This is because criminal-history data collection for the national CRIS starts at much later stages of the criminal process, meaning the CRIS is of less use for criminal investigations. In Germany, in addition to police databases, there is a centralized register of ongoing prosecutions that is completely separate from the national CRIS. The register's purpose is primarily to coordinate the work of prosecutors' offices and to avoid the duplication of efforts. The U.S. also maintain a series of additional information systems, separate from the national CRIS, whose primary purpose is to assist law enforcement agencies, such as the National Crime Information Center.

By contrast, in Australia, Canada, and England and Wales, there is no separate national-level police information system. In England and Wales, the CRIS also functions as a national-level repository of police information. A similar situation exists in Canada, where the CRIS is a constituent part of CPIC, a central database supporting Canadian law enforcement. In Australia, where police information is predominantly maintained by local and/or state-level agencies, the national-level CRIS serves the function of facilitating the retrieval of data from subnational information systems.[150]

These organizational differences across the countries are also reflected in whether the national CRIS is linked with other data repositories. The German system does not have any links with other databases; in the Netherlands, the JDS is linked to the WODC (its copy maintained for research purposes) but not to any other databases. In the remaining countries (Australia, Canada, England and Wales, and the U.S.), links to originating state systems or other databases, such as fingerprint systems, are found.

[150] This is similar to a function provided by CPIC, which tells users which local law enforcement agency may hold additional information that has not been provided to CPIC.

Table 7.1. Comparison of the Systems' Main Characteristics

	Germany	Netherlands	Canada	England and Wales	Australia	United States
Name of the system	BZR	JDS/OBJD	CPIC	PNC	NPRS	Next Generation Identification (NGI)
Type of system	Centralized repository of criminal records	Centralized repository of criminal records	Centralized repository of criminal records	Centralized repository of criminal records	Centralized repository of criminal records	Centralized repository of criminal records
Contents	Court convictions (and public prosecutor and court disposals of juvenile cases)	Criminal history of people who have been prosecuted	Criminal history of people who have been charged with an offense	Criminal history of people who have been arrested for a recordable offense, as well as such noncriminal-history information as banning orders, driving disqualifications, or gun owner registration	Some variation in what is input across police jurisdictions; typically criminal history of people who have been arrested for an offense	Criminal history of people who have been arrested and/or convicted
Governing laws	BZRG	Dutch Code Concerning Data Used in Judicial Settings and Criminal Proceedings; Judicial Data Act	Identification of Criminals Act, Criminal Records Act and the Youth Criminal Justice Act	Police and Criminal Evidence Act 1984	Australian Crime Commission Act 2002; relevant state-level legislation	Various U.S. Code provisions and the Code of Federal Regulations; relevant state-level legislation
Managed by what agency	BfJ	JustID (of the Ministry of Justice and Security)	RCMP	PNC Bureau, although each police force is responsible for the data they input	ACIC	FBI
Data provided by what agency	Courts and other reporting authorities	Primarily prosecutors and courts	Police agencies	Primarily police agencies, as well as courts, ACRO Criminal Records Office	Police agencies	State, tribal, territorial, and federal agencies (e.g., law enforcement, courts, corrections, and probation)
Who owns the data?	BfJ	JustID	Originating agencies	Originating agencies	Originating agencies	Originating agencies
Is the CRIS centralized, or does it link to other external CR data locations?	Centralized	Centralized	Centralized	Centralized	Both	Both
Linkages with other databases	None	Yes (between JDS and WODC)	Yes	Yes	Yes	Yes, to state repositories and interoperability with other federal systems

Content of National Criminal Record Information Systems

The variation in the content of national CRIS in the countries covered in this report mirrors the differences in what type of agency is responsible for maintaining the national system, as discussed above (see Table 7.2). In Australia, Canada, England and Wales, and the U.S., law enforcement agencies are the creators of criminal records as well as one of the primary (although not necessarily the only) sources of data for the national CRIS. In Australia,[151] Canada, and, in some instances, England and Wales, police agencies are responsible even for the provision of data originated by other criminal justice agencies, such as court dispositions. By contrast, in the Netherlands and Germany, each country's national system primarily relies on data from public prosecutors and courts, respectively, although as in the other countries, additional agencies also provide information to the system.

Some variation exists also with respect to what offenses are to be reported to the national CRIS. In England and Wales, recordable offenses are generally defined as those that could result in imprisonment.[152] In Canada, there is no formal requirement to report any information other than data on serious juvenile offenses. In practice, however, Canadian agencies typically report all serious offenses (defined as those punishable by more than a small fine or a short custodial sentence) and may also report data on less serious offenses. In Germany, all court convictions and administrative rulings (e.g., a ban on certain professions) are recorded.[153] In the Netherlands, all crimes and most misdemeanors are captured in the national system. In the U.S. and Australia, the decision on which offenses get reported to the national system rests with individual states and/or, in the U.S., federal agencies. These rules illustrate the range of information collected in the national information systems. On one end of the spectrum, Australia, Canada, England and Wales, and the U.S. start recording data early in the individual's engagement with the criminal justice system. On the other end of the spectrum, the Netherlands and Germany do not create a record unless the case has progressed in the system to a certain milestone, either to prosecution (in the Netherlands) or to conviction (in Germany).

Criminal-history records in all the countries contain the following information: personal information, such as name(s), date and place of birth; information on the offense, such as date and applicable legal provisions (e.g., charges and statutes); and information on the sentence imposed, including any suspensions, conditions, and subsequent modifications. However, within these categories, some variation and unique features can be observed. In Australia, Canada, England and Wales, and the U.S., the national systems include physical descriptors, such as

---

[151] Australian courts provide information to the local police information system (though sometimes the police have to process the submission manually). The entire police record then gets uploaded to the national system.

[152] Other noncriminal reasons may also lead to the creation of a record in the national system.

[153] In addition, disposals of juvenile cases for public interest reasons (with or without the imposition of a condition) are also recorded.

tattoos or body marks, which may be useful for criminal investigations. A similar distinction can be made with respect to biometrics. In Germany and the Netherlands, the law does not permit the storage of biometric information in the national CRIS. Criminal justice agencies in those countries may collect biometric data and store them in other databases; however, this information would not be directly linked to the national CRIS. By contrast, the national CRIS in the other countries either directly contains biometric information (fingerprints in Canada and the U.S. and photographs in Australia and the U.S. when provided by the originating agency) or provides links to other databases where this information is stored (e.g., links to national DNA databases in England and Wales and in Australia).

Data Transfer

In all the countries, data are generally provided to the national CRIS by originating agencies via a standardized electronic reporting system, although some manual input may take place in limited circumstances in England and Wales, the Netherlands, and the U.S.[154] In all countries except the U.S., data provision from originating agencies to the national CRIS takes the form of a data transfer to a centralized repository rather than just a submission of a link to the originating agency's own information system. With the exception of Australia, this means that once a criminal record has been transferred to the national CRIS, its retention in the national system does not depend on whether it is also retained in the information system of the originating agency. Australia is an exception to this rule as the content of the national CRIS is refreshed on a daily basis as an extract of the pertinent information held by contributing police agencies. Therefore, if a contributing agency modified or deleted an existing record it holds, this change would be automatically reflected in the next refresh of the Australian system. In the U.S., some information is transferred to the national repository, and some is retained only in state databases but made available via the national system.

In all the countries, the information submitted to the national system typically does not represent the totality of data pertaining to the criminal record that are held by originating agencies, although the extent of this phenomenon varies across countries. For instance, the Australian system is focused on criminal-history information and may not include further details on the person or incident in question. Similarly, Canadian police agencies have the discretion to decide how much additional police information to provide to the national system. In these instances, the national systems will provide users with an indication of which agency to consult in search for information that may not be available via the national system. Furthermore, in countries where not all offenses are required to be reported to the national system, there may be a discrepancy between the content of the national CRIS and local repositories. This situation may also affect the use of national systems for civilian purposes. For instance, in Canada, criminal

[154] In Australia and Canada, in some instances police agencies may need to manually process information received from other agencies, notably the courts. The subsequent transfer to the national repository is automated.

background checks required for work in vulnerable sectors mandate that, in addition to a search of the national system, local police records be consulted. This arrangement reflects the fact that local databases may contain criminal-history information that is not available from the national system.

Data Retention

Data retention policies are another area where there is variation across the countries. Germany and the Netherlands differ from the other countries and may retain data for a comparatively shorter period. In Germany, the length of the retention period depends on the sentence imposed, with the rule that longer sentences are generally associated with longer retention periods. In the Netherlands, the length of the retention period depends on the offense, with a similar rule that records for more serious offenses are retained longer. This means that, in both countries, an individual's criminal-history information for an offense is removed after the expiration of the retention period if they do not commit another offense during its course.[155] By contrast, in the other countries, criminal records will generally be retained for a much longer period—countries either set an age limit that substantially exceeds the country's life expectancy (125 years in Canada, 110 years in the U.S., and 100 years in England and Wales) or routinely do not delete criminal records at all. In Canada, however, this rule applies only to conviction records, which are subject to the 125-year-old rule. Discharges (court dispositions involving a finding of guilt but imposing no sentence) are retained for a much shorter period, depending on the severity of the offense. Nonconviction data are not covered by any formal rules at the national level. This makes Canada the only country in this report where the retention policy for nonconviction information is different from that for other court dispositions. Germany does not have any retention policy for nonconviction information because, as discussed above, only data on convictions and administrative rulings (e.g., a ban on certain professions) are recorded.[156]

Canada and Germany have a different data retention regime for juvenile criminal records compared to adults.[157] While the arrangements in both countries differ in concrete details and time frames, the operating principle is similar. Juvenile records are retained only for a limited period, after which they are no longer visible to users of the national CRIS as long as the individual does not commit another offense. There is, however, one point of divergence between the two countries. In Germany, juvenile records are deleted from the system after the age of 24.

---

[155] In Germany, a few exceptions are not covered by this rule and are not subject to deletion on the condition of no further criminality. In the Netherlands, a pseudonymized version of the record will be retained in a copy of the national CRIS that is used for research purposes.

[156] Information on public prosecutor and court disposals of juvenile cases is also recorded.

[157] The definition of juveniles in Canada is ages 12–17 and in Germany ages 14–17. In addition, in Germany, young adult offenders (ages 18–20) are required to be processed under juvenile criminal law if they are considered to be juvenile in terms of their development or if the offense was a transgression of a juvenile nature.

In Canada, juvenile records are rendered inactive but could be reactivated in the event of subsequent criminality.[158] Furthermore, Germany has different arrangements for juvenile and adult criminal records from the perspective of access rules and disclosure requirements. The national CRIS in the other countries (Australia, England and Wales, the Netherlands, and the U.S.) treat adult and juvenile criminal records the same way.

Canada, Germany, England and Wales, and the U.S. allow for the removal of criminal records from national systems before any formal conditions for expungement are met. In Canada and Germany, individuals may apply to a national authority (PBC and the Ministry of Justice, respectively) to render a conviction record invisible on any searches of the national CRIS. If granted, the record will be suspended in Canada (i.e., retaining the possibility of reactivation if the conditions of the suspension are violated). In Germany, the record will be deleted without the possibility of reversal. In England and Wales, individuals can apply to the agency where their criminal record originated to have the information deleted from the national system; this option is applicable only to noncourt disposals (e.g., cautions) and nonconviction records and cannot be used for conviction data. Similarly, individuals with a nonconviction criminal record in Canada can apply to the arresting police agency to have the record deleted. If granted, the arresting agency will then instruct the national authority to also delete the record from the national system, although the RCMP, the owner of the national system, may refuse to do so. In the U.S., records held in the national system may be deleted earlier if instructed to do so by originating agencies. There are no provisions for the early deletion of criminal records in Australia and the Netherlands.

The national systems in all the countries also vary depending on whether records that have reached the end of their retention period are deleted or are rendered invisible but could be reinstated for any reason. In the U.S., England and Wales, and Germany, the deletion is final and does not allow any subsequent reinstatement or recall of the information. In Canada, adult criminal records marked for deletion are also completely removed from the system, whereas juvenile records are sequestered, with the possibility of their reactivation. In the Netherlands, criminal records for which the retention period has expired are filtered out so that they do not appear on any search of the system but continue to exist. However, there is no legal reason for their potential reactivation; expired records are retained solely for research purposes. In Australia, records are not actively deleted by the owners of the national system; instead, deletion is achieved when the originating agency removes a record in its own system and this change is reflected in the daily refresh of the national system.

[158] This option is open for five years, unless it was a serious violent offense for which an adult sentence was sought, in which case the period is indefinite.

Table 7.2. Comparison of the Systems' Content

	Germany	Netherlands	Canada	England and Wales	Australia	United States
Name of the system	BZR	JDS/OBJD	CPIC	PNC	NPRS	NGI
What information is collected?	Court convictions (and public prosecutor disposals of for juvenile cases)	Criminal history of people who have been prosecuted	Criminal history of people who have been charged with an offense	Criminal history of people who have been arrested	Criminal history of people who have been charged with an offense (although some variation across police jurisdictions)	Criminal history of people who have been arrested/convicted
Personal information	Name(s), gender, address, nationality, and date and place of birth	Name, place and date of birth, BSN, address, and citizenship	Names and aliases, date and place of birth, gender, physical descriptors, and race	Nominal data (including name, date of birth, sex, skin color, height, and any other identifying details), warnings, and identification numbers; note if there is a record generated by IDENT1	Name and other identity information, such as date and place of birth	Biographic information (e.g., name, date of birth, height, weight, Social Security number, sex, and race)
Information on offense/sentence	Yes	Yes	Yes	Yes	Yes	Yes (if provided by the owning agency)
Biometrics (if not, why not?)	No, not permitted by law	No, not allowed by law	Yes, fingerprints (DNA on some individuals held in a separate database)	Yes, links to NDNAD and IDENT1 records, where they exist	Yes, photographs of the individual and links to biometric data in NAFIS and NCIDD, where they exist	Yes, fingerprints and may include palmprints and photographs if provided by the originating agency
When does data collection begin? (e.g., arrest or conviction)	Court conviction (for adults); court/prosecutor disposals (for juveniles)	Case registration with the prosecutors' office	Arrest	Arrest	Varies according to police jurisdiction	Arrest
Who provides the data?	Courts and other reporting authorities	Primarily prosecutors and courts	Police agencies, which are also updated with court data	Primarily police agencies, as well as courts and ACRO Criminal Records Office	Police agencies, which also are updated with court data	State, tribal, territorial, and federal agencies (multiple types of agencies, e.g., law enforcement, courts, corrections, and probation)

Is the transfer process standardized across contributing agencies?	Yes, via an automated reporting procedure	Typically yes (either electronic messages or online upload)	Yes, data provided in a standardized electronic form	Yes, with small variations in manual/electronic inputting	Yes, with some variation in the amount of information transmitted to the NPRS across police jurisdictions	Yes, data provided in a standardized electronic form and other forms as approved by the FBI
Data retention period	5–20 years for adults (depends on the sentence) unless the person reaches 90 years or dies sooner; at 24 years of age for juveniles	5–80 years (depends on the offense); retained indefinitely in a research copy of the JDS	Depends on the disposition: adult convictions until 125 years, discharges for 1–3 years, and no formal rules on nonconvictions	Until individual's 100th birthday	A matter of legislation of relevant police jurisdiction; in practice, information not routinely deleted	Up to 110 years of age (biometrics may be deleted earlier); removed if instructed to do so by the record-owning agency
Differential data retention regime for juveniles?	Yes	No	Yes, records not available after 3–5 years (convictions), 1–3 years (discharges), or immediately (most nonconvictions)	No	No	No, unless removal of information is required by statute
Differential data retention regime for nonconvictions?	Non-convictions not recoded	No	Yes	No	No	No
Where data are mandated to be deleted at the end of the retention period, is the deletion final?	Final but not automatic	Not final; there is a theoretical way to renew expired records although there is no legal basis for doing so	Yes, for adults; juvenile records sequestered	Yes	No	Yes
Possibility of shielding data?	Yes, individuals may apply to have their record deleted earlier	No	Yes, after a certain period, individuals may apply for a pardon (shielding of a record from being visible during searches)	Individuals may apply to chief officer where record originated to have noncourt disposals (such as cautions) and nonconviction outcomes from their records deleted	Yes	Records may be sealed if requested by the owning agency (in accordance with state laws)
Volume of data held	4.3M people; 16M dispositions (2018)	2.75M persons (2017)	4.25M records; number of unique individuals unclear (2018)	10.5M individuals (2014)	11M records; number of unique individuals unclear (2018)	72M fingerprints (2016)

Access to the System

Operational Access

Across all the countries, access to criminal-history information systems is granted to law enforcement and other criminal justice agencies to support their operations (see Table 7.3). Under certain conditions, access may also be provided to other selected government agencies, although the extent of this provision varies across the countries. For instance, Australia maintains a relatively restrictive access regime, with only a small number of non-law-enforcement agencies able to access the national system. By contrast, the number of agencies with some form of access rights to the Canadian NRCR exceeds 3,000.

Provisions also exist for the international sharing of data, for instance with Interpol or with selected agencies from neighboring countries (e.g., some U.S. agencies have access to Canadian NRCR data). Across the focus countries, one of the most advanced and formalized frameworks for cross-country sharing of criminal-history data is established in the European countries, which are able to use ECRIS. This system obliges EU member states to notify other member states regarding the criminal history of their citizens and to respond to queries received from other member states. These exchanges of information make use of reference tables for offenses and sentences, which serve to approximate the criminal laws of individual member states.

The identity of a given user agency can have two implications in terms of access rights to national criminal-history databases. First, it frequently determines what type of information they can access, with certain content available only to specific agencies. To illustrate, in Germany, access to information on juvenile noncustodial sentences is afforded to a very small number of users. Second, the identity of a given user agency may determine whether they can edit existing criminal records held in the national system or are restricted to read-only privileges, which tends to be common particularly for non-criminal-justice agencies. For instance, in Canada, records in the NRCR can be edited only by the RCMP, although some agencies may edit information in CPIC's other information data banks, which complement the NRCR. Electronic access is the predominant form of querying existing systems in all the countries, although some paper-based communication persists to a limited extent. To demonstrate the variability described above, the remainder of this section provides a brief overview of the main access arrangements in each country.

Germany

In Germany, a number of government institutions and agencies have access to the full database, such as criminal investigation units in police departments; courts, public prosecution, and supervision authorities; secret services; financial and tax authorities' criminal investigation departments; naturalization services; authorities dealing with foreigners; and specialized administration agencies. Direct access to the BZR is prohibited; agencies that wish to view

information held in the system must submit an electronic request to the BfJ. There are a number of restrictions on the level of access to the information held in the BZR. For example, records pertaining to drug-treatment orders are available only to courts and prosecutors; access to records relating to juvenile prison sentences may also be limited in this way. Furthermore, as discussed above, there are strong restrictions on sharing records relating to juvenile noncustodial sentences.

The Netherlands

In the Netherlands, law enforcement and other agencies that contribute to the JDS are authorized to access the system for operational purposes. In addition, other public authorities, such as local authorities, may be granted access to JDS data under specific regulations. Specific, granular conditions of data access by individual organizations (including type of data, purpose of data access, preconditions of access, data retention, and sharing with third parties) are frequently addressed by secondary legislation. Information from the JDS can be accessed multiple ways. Authorized users external to JustID can query the system via the online interface JD-Online, through a messaging application, or via electronic message traffic (e.g., XML). Some users (such as municipalities) are provided information in hard copy, although hard copies are being phased out.

Canada

Access to Canada's CPIC is granted to over 3,000 designated CPIC agencies, including Canadian law enforcement agencies, federal and provincial agencies with limited law enforcement power, and agencies with roles that support law enforcement. Access is also granted to international partner agencies, including Interpol and certain U.S. agencies at the federal and state levels. To gain access to CPIC data, agencies need to complete a memorandum of understanding with the RCMP, and access arrangements may differ depending on the type of user agency. Access to and use of CPIC is tracked, and resulting metadata are stored by the RCMP. In undertaking searches of the NRCR for operational purposes, user agencies can access three layers of data, depending on what query they decide to run: CRII, the most complete set of information; CRS, a summary version of information held by CPIC; and Criminal Name Index (CNI), a list of names of individuals for whom there may be an existing criminal record in the repository.

England and Wales

In England and Wales, the PNC is used by law enforcement agencies across the UK to share information and facilitate criminal investigations. In addition, approximately 60 organizations (many of which are agencies within the Home Office) have read-only access to information on the PNC to help them fulfill their statutory functions and will either link their systems to it or derive information from a read-only access portal. The PIAP, a centralized group comprised of a cross-section of representatives from different forces, considers requests for access to the PNC.

Any organization given access will be asked to sign a code of connection and a supply agreement, which sets out the purpose of the application, the people who will have access to the data, requirements around the security environment, and other terms of access. Access is usually granted on a permanent basis, although some arrangements can be temporary. Non-law-enforcement agencies can request data for a specific individual but cannot themselves make any additions or edits to the records, although nonpolice prosecuting agencies may request that ACRO Criminal Records Office create a PNC record for a defendant. Information relating to an individual's criminal history may also be shared with international partners, on request.

Australia

Australia's NPRS is used by law enforcement agencies nationwide to share and access information on persons of interest and to facilitate criminal investigations. In addition, there is a small number of non-law-enforcement agencies that can access the NPRS directly, although only to extract the information they need for their operations. ACIC have recently developed a limited-view functionality so that it is easier to facilitate access to some but not all records or parts of records for these agencies with access to the NPRS. Courts and corrections agencies generally cannot access the NPRS or link to it directly; in general, any criminal-history information that courts and corrections agencies require for an individual is supplied by the local police force. There is no direct access to the NPRS from outside of Australia. However, such agencies as Interpol, along with regional policing partners, may receive information from the NPRS in relation to criminal investigations or following a deportation order. Furthermore, some agencies may partner with state police agencies for investigations and be able to access information relating to the individuals involved.

United States

Finally, access to the U.S.'s NGI System is granted to law enforcement and criminal justice agencies, including prosecutors and courts. Access is requested electronically, through a direct query of III or a fingerprint submission to the NGI System. III queries are conducted on the basis of any of the following items (or their combinations): biographic descriptors, a state-assigned identification number, or a unique identifying number assigned to the individual by the FBI. III enables individual states to respond directly to the requestor; in situations where the state is unable to provide a response, the FBI will do so. These situations include queries pertaining to federal offenders, individuals arrested outside of III states and territories, and arrests not supported by III states. For a fingerprint query resulting in a positive match, the national repository will determine which agency (i.e., the FBI or a state) is responsible for maintaining and disseminating the record in question. In the event of a negative fingerprint match, a new record is created in the national system using the arrest details from the submission. The submitting agency or another related agency is required to submit subsequent updates to the record. As with the other countries included in this study, the level of access granted depends on

the type of user agency requesting it and on applicable laws (federal and state). All requests for information need to be accompanied by a justification, and the FBI keeps an audit trail of all disclosures. Where appropriate, agencies accessing national criminal-history information must have an executed user agreement with the FBI.

Table 7.3. Comparison of Arrangements to Access Criminal-History Data for Operational Purposes

	Germany	Netherlands	Canada	England and Wales	Australia	United States
Name of the system	BZR	JDS	CPIC	PNC	NPRS	NGI
Who has access?	Criminal justice bodies, other selected public authorities, and EU partners	Criminal justice bodies, other selected public authorities, and EU partners	Law enforcement, agencies with limited law enforcement powers, agencies supporting law enforcement, and international partners	Law enforcement and criminal justice bodies, other selected public authorities, and international partners	Law enforcement agencies across Australia, and very few non-law-enforcement agencies	Law enforcement, criminal justice agencies, and other authorized agencies
On what basis?	To inform work of criminal justice agencies as well as other authorities (e.g., to vet personnel)	To inform work of criminal justice agencies as well as other authorities (e.g., to vet personnel)	To support user agencies' operations	To support user agencies' operations	To support user agencies' operations	For criminal justice purposes (e.g., law enforcement, investigators, prosecutors, and courts)
How is access facilitated?	Through an electronic request to the BfJ (no direct access allowed)	Mostly electronically (either online search interface or message traffic)	Electronic access; nonpolice agencies need memorandum of understanding with the RCMP	Electronic access; nonpolice agencies may have read-only access or receive a data extract from the PNC	Direct or limited-view access	Electronic requests through a direct query of III or a fingerprint submission to the NGI system
Any limitations on who can see what?	Yes, records pertaining to drug-treatment orders and juvenile prison sentences can be made unavailable to authorities other than courts and prosecutors; strong limitations on sharing records on juvenile noncustodial sentences	Yes, access by concrete organizations subject to agency-specific conditions	Yes, level of access depends on the type of user agency	Yes, level of access depends on the type of user agency	Yes, level of access depends on the type of user agency	Yes, level of access depends on the type of user agency

Civilian Access

All the countries allow individuals to check their own record for information held about them and provide background checks for such purposes as employment, visa applications, and adoption applications (see Table 7.4). Individuals in all the countries can file an application for a record check, either with the system operators directly or via accredited checking agencies. For all the countries, the level of disclosure may depend on the offense history and the type of check being performed. For example, in Germany, offense histories will appear on a check only for a limited period, depending on the sentence. Furthermore, juvenile noncustodial data and adult convictions leading to only minor sanctions do not appear in check certificates at all. In the Netherlands, even the existence of a criminal record may not prevent an applicant from obtaining a clean check if the deciding authority determines that the criminal record is not relevant for the purpose of the application. In addition, countries performing criminal-history checks offer enhanced versions for individuals intending to work with children or vulnerable people. These enhanced checks can involve more thorough searches of existing data or be subject to stricter disclosure rules. For instance, in Australia, an individual who is seeking to work or volunteer with children or other vulnerable populations is required to apply for a working-with-children check, which may disclose criminal-history information that would not be shared in a regular employment check, and may check other information systems beyond the NPRS, such as court databases (for prosecutions brought by nonpolice agencies) and professional malpractice record systems. In Canada, a vulnerable-sector check must involve a search of local police databases, which may contain information not available from the NRCR.

Table 7.4. Comparison of Arrangements to Access Criminal-History Data for Civilian Purposes

	Germany	Netherlands	Canada	England and Wales	Australia	United States
Name of the system	BZR	JDS	CPIC	PNC	NPRS	NGI
Who has access?	Individuals can check their own record or apply for a certificate of conduct	Individuals can check their own record or apply for criminal check certificate	Individuals can check their own record or apply for criminal check certificate	Individuals can check their own record or apply for criminal check certificate	Individuals can check their own record or apply for criminal check certificate	Individuals can check their own FBI record by submitting a Departmental Order 556-73 request
On what basis?	To check what is being held on them and for employment/background verification purposes	To check what is being held on them and for employment/background verification purposes	To check what is being held on them and for employment/background verification purposes	To check what is being held on them, for employment/background verification purposes, and to work or move abroad	To check what is being held on them, for employment/ background verification purposes, and to work or move abroad	To check what is maintained by the FBI and for authorized non-criminal-justice purposes (e.g., employment and licensing)
How is access facilitated?	Individuals file an application	Individuals file an application	Individuals file an application	Individual applies for a check conducted by DBS or ACRO Criminal Records Office	Individual applies to the National Police Checking Service or an accredited checking agency	Individuals can request a copy of their own FBI record by submitting the necessary information to the FBI
Any limitations on who can see what?	Yes, criminal records are eligible to appear on a certificate of conduct for a limited period (3–10 years, depending on the sentence); juvenile noncustodial data and minor adult sanctions do not appear on the certificate of conduct	No limitations on who can see what, but the processing agency determines what is relevant to include in a criminal check based on the nature of the application	No limitations on who can see what, but level of disclosure depends on the type of check performed	Level of disclosure depends on the offense history and the type of check performed	Level of disclosure depends on the offense history and the type of check performed	Level of disclosure depends on the purpose of the request as well as federal and state statutes

Researcher Access

Access to criminal-history data is granted to researchers in all the countries included in this study, although the level of access varies widely (see Table 7.5). Typically, access may be approved for specific research activities that may generate knowledge and inform practice or policymaking, although there are no such explicit limitations on the purpose of research using criminal-history data in the Netherlands. In Germany, requests for BZR data have so far been granted only to German researchers with the backing of an established research institute or university, as the Ministry of Justice cannot control data protection agreements and facilities in other countries. Both Canada and Australia restrict research access to researchers working within or on behalf of the government; for Australia, this means only researchers from the Australian Institute of Criminology, while Canada facilitates access to information for researchers working in or on behalf of a police agency, provincial or federal attorneys general, the solicitor general, or the minister of justice. The Netherlands and England and Wales place no explicit restrictions on the type of researcher who may apply for access to criminal-history information, although applications are subject to approval by the countries' respective review panels and boards. In the U.S., the FBI also has a review board that ensures the requestor and the purpose of the request are authorized pursuant to federal statutes governing the use of criminal-history information for research purposes.

There are considerable differences in approaches to the level of access researchers may be granted. Canada places no a priori limitations on what researchers may see. In the Netherlands, researchers have access to a pseudonymized database. In England and Wales, names may sometimes be redacted from data shared with researchers while data shared with researchers in Australia are always anonymized. In Germany, the BfJ can transmit nonanonymized data from the BZR to universities or other research institutes for research projects if the use of anonymized data is not possible and the public interest in the research outweighs the interests of the persons concerned; anonymized data may also be shared if these conditions are not met. Finally, restrictions on the type of access researchers may receive in the U.S. are determined by the FBI and the existing federal statutory authority.

Table 7.5. Comparison of Arrangements to Access Criminal-History Data for Research Purposes

	Germany	Netherlands	Canada	England and Wales	Australia	United States
Name of the system	BZR	OBJD	CPIC	PNC	NPRS	NGI
For research purposes, who has access?	German-based researchers and research institutions	Approved researchers	Researchers working in or on behalf of a police agency or selected authorities	Approved researchers	Researchers within the Australian Institute of Criminology	Researchers as authorized by the FBI IRB and Office of the General Counsel pursuant to existing federal statutory authority
On what basis?	To inform legislative or administrative policy proposals	No explicit limitations	Research on the execution or administration of the law, including evaluation of treatment or correctional programs	The research must offer a demonstrable benefit to the Ministry of Justice in generating knowledge, and the data must be used for statistical and research purposes only	For specific research projects conducted by AIC researchers	For research projects that meet the FBI IRB criteria and existing federal statutory authority
How is access facilitated?	Via an application outlining the research project and the need for BZR data	Via an application to the WODC (a research arm of the Ministry of Justice)	Via an application with the RCMP or another user agency	Via an application to the MIAP	Request to ACIC	Via a written request to the FBI IRB
Limitations on who can see what?	No a priori limitations, subject to approval (though approval is historically granted only to German-based institutions)	No a priori limitations (though data already pseudonymized), subject to approval	No a priori limitations, subject to approval	Yes, names of individuals may be redacted	Yes, data anonymized	Yes, determined by the FBI IRB and existing federal statutory authority; transfer agreements are executed

Data Quality and Completeness

Across the countries, there are common challenges with achieving data quality and some that are specific to the jurisdiction (see Table 7.6). In Australia, Canada, England and Wales, and the U.S., ensuring the quality of data held in the systems is the responsibility of the agency that originally entered the information. However, in Germany and the Netherlands, this responsibility rests with the agency that maintains the centralized system—the BfJ in Germany and JustID and the WODC in the Netherlands—although in both countries the central authorities work with the originating agencies to resolve any identified data issues.

Challenges with Data Quality and Completeness

Overall, four types of data quality and completeness challenges were identified across the countries: issues with data collection, issues with data transfer, technological issues, and issues with scope of collected data. In Australia, the U.S., and Canada, similar challenges relating to complexities of gathering data from multiple state and local jurisdictions have been experienced, such as variable formats in the U.S. and variation in the type of information that state and territorial agencies share with the centralized system in Australia. In addition, multiple records relating to the same person but originating from different jurisdictions can be found in Australia. In Canada, variation in recording practices by local law enforcement agencies also occurs, although frequently in the context of police data that may not always be submitted to the national system.

A second challenge is the transfer of data from originating agencies to the national system. For instance, in the Netherlands, inaccuracies during the receipt and registration of criminal-history information from originating agencies were identified as a data quality concern. Issues may arise in later stages of data transfer as well. In the U.S., missing dispositions have been identified as an issue, as have delays in uploading information from law enforcement agencies to the national system in Canada.

Third, aging technological infrastructure can also represent a challenge. This has been a concern noted in the UK, but examples can be found in other contexts as well, for instance, in the form of reliance on paper-based records and communications in a small number of instances in the Netherlands, which is being phased out.

Lastly, the fourth issue is the limited scope of information held in national systems. In Germany, a key challenge for users is presented by the limited scope of the information captured in the system: typically only records relating to the most serious offenses are retained in the long term, and cases that were dismissed by public prosecutors or courts are not recorded in the system. Furthermore, searches of the system must be done by name, as no biometric identifiers are included. In Canada, local agencies also have some latitude in terms of what information they provide to the national system, which could theoretically give rise to unevenly complete criminal

records. However, issues pertaining to the scope of information recorded are products of the legal framework governing the respective national systems and do not represent deficiencies on the part of the system's functioning or that of its users.

Efforts to Ensure Data Quality

A variety of approaches to ensuring data quality in these systems were identified, often driven by the nature of the data quality issues experienced in each jurisdiction. The first group of efforts revolves around checking the accuracy and quality of submitted data. To illustrate, for Germany and Australia, the automated transfer of data from originating agencies (thereby minimizing the need for further processing of received data) has been noted as helping to reduce the risk of human error in entering the information. In England and Wales and the U.S., the police use fingerprint records to positively identify an individual in the system. In the U.S., an issue with a fingerprint submission will trigger rejection and/or an error message to the contributing agency, while in England and Wales incomplete information entered into the system is automatically flagged for the attention of the data entry officer. Similarly, if an update from the court system in England and Wales cannot be matched with the relevant criminal record, an alert is automatically transmitted to the originating law enforcement agency for manual correction. In the Netherlands, JustID is tasked with investigating and rectifying registration errors in the JDS. Lastly, all the countries allow individuals to review their own records and submit a correction if they believe their data has been wrongly recorded or is incorrect.

The second group of efforts addresses issues with data transfer and gaps in the provision of information from originating agencies. In Canada, efforts have been made to facilitate faster electronic submission of data to address the delay in uploading information onto the NRCR. In the Netherlands, JustID initiated a project called Focus on Data Quality, which focuses on monitoring and identifying potential improvements to messaging traffic to the JDS and comparing JDS data with source files. It also led to the establishment of a virtual data quality office, bringing together the main stakeholder agencies working with criminal-history data. In the U.S., improvement efforts have been centered on identifying missing dispositions and standardizing rap sheets.

All the countries have put in place processes to audit the quality of the data held in the centralized systems. In Germany, new records are automatically checked for errors in data entry, and errors are followed up with the originating agency; in the Netherlands, the WODC conducts checks when new data are added to the OBJD and the system is refreshed, and verifications are performed with respect to data counts and potential duplicate cases. In Canada, Australia, and England and Wales, personnel in each law enforcement agency are tasked with auditing data entry and use by that agency. In Canada, quality assurances review reports are regularly distributed to police chiefs; similarly, in England and Wales, HMICFRS conducts audits of data quality and usage. In the U.S., the FBI conducts audits of each state central repository and other agencies with direct access to criminal-history information in III.

Table 7.6. Comparison of Selected Aspects Related to Data Quality and Completeness

	Germany	Netherlands	Canada	England and Wales	Australia	United States
Name of the system	BZR	JDS/OBJD	CPIC	PNC	NPRS	NGI
Entity responsible for data quality	BfJ	JustID, the WODC	Originating agencies	Originating agencies	Originating agencies	Originating agencies
Challenges related to data quality and completeness	Limited scope of the information captured in the system	Inaccuracies during receipt and registration of data from originating agencies	Delay in the transfer of information from police agencies to the RCMP (officially documented) and variation in recording practices by local police	Advanced age and technological limitations of database; some information must be entered manually; and inconsistency in pre-2006 records still retained in the PNC	Absence of identity resolution creating multiple records for individuals; delays in receiving court data; some information must be entered manually; and some variation in information transmitted across police jurisdictions	Missing dispositions and variable rap-sheet format
Notable features to help ensure data quality	Automated data transfer	Virtual data quality office linking main originating agencies	Efforts to enable faster electronic submission of information	Police almost always enter data into the PNC, as they have access to fingerprint records to prove the identity of an individual in the system; and automatic alerts when data is entered inaccurately/incompletely	Mostly automated data transfer	Correlation between state-held and FBI-held records; audits; and improvement efforts around missing dispositions and standardization of rap sheets
Processes to audit data quality	Automatic quality checks of received data	The WODC performs data verification and checks at every refresh (quarterly)	Regular quality assurance review reports distributed to Canadian police chiefs; and personnel on each force who audits data entry and use by that force	Personnel on each force who audits data entry and use by that force; and HMICFRS audits	Personnel in each agency who audits data entry and use by that force	FBI conducts an audit of each state central repository and other agencies with direct access to criminal history maintained in the III

Concluding Remarks

There is considerable variation across the countries in this study in how they approach the collection, management, and use of criminal-history information through their national information systems. Notable areas of divergence include, but are not limited to, the scope of criminal-history data collection, retention of criminal-history information, and access arrangements both for operational and civilian purposes. These differences help shape how criminal-history data can inform the work of various criminal-history agencies and their partners, as well as help support the rehabilitation of individuals involved with the criminal justice system. Information systems that begin collecting data at earlier stages of individuals' involvement with the criminal justice system and/or retain data for longer periods of time are in a position to provide criminal justice agencies with a larger volume of information. This can in turn help inform such areas as law enforcement, criminal investigations, and sentencing decisions. At the same time, large-scale data collection and/or retention may be more likely to raise privacy and fundamental rights questions, particularly insofar as nonconviction data are concerned. By contrast, systems with more restrictive data collection and dissemination rules may be more likely to help foster the rehabilitation and reintegration of individuals involved with the criminal justice system.

At the same time, a series of commonalities should also be noted. Across all the countries, a trend toward greater automation and standardization can be observed, closely linked with efforts to improve data quality and completeness. Relatedly, several countries have recently launched initiatives dedicated to addressing deficiencies and challenges pertaining to data quality.

The in-depth, comparative analysis of the countries' approaches to criminal-history information presented in this report has highlighted innovative practices that could be adopted elsewhere to improve the functioning of these systems. These practices are discussed in detail in the individual country chapters and include the Dutch practice of maintaining a copy of the national criminal-history database that is dedicated to research purposes, enabling criminal-history data to be available for scientific work in perpetuity while safeguarding the rights of individuals with a criminal record. Also of note is the legal and technological solution created to allow the transmission of criminal-history data among EU member states via ECRIS. This represents a harmonized framework for information exchange across jurisdictions with different legal traditions and arrangements with the help of common reference tables of offenses and sentences.

Appendix A. Country Chapter Outline

1. Brief overview of the country and criminal justice system
   - Type of government (e.g., unified or federal/state)
   - How criminal justice system is structured
   - Size of the criminal justice system (per capita arrests, inmates, and those subject to community corrections)
   - Terminology relevant for understanding how criminal justice system operates
2. Understanding the national criminal-history record system(s)
   - Name of the main database
   - Is it a separate database, or are data pulled from subnational sources?
   - Who owns/maintains/pays for the database, and what regulations govern its use?
   - Information entered into the national criminal-history record system
     - Details of the information stored (e.g., name, date of birth, address, arrests, convictions, sentences, probation violations, and biometric measures)
     - Size of the system (e.g., number of records)
     - Include flowchart showing when data are collected, when they are transferred, and where they are stored (note such issues as paper/electronic submission)
   - Is reporting required, incentivized, or automated?
   - Data retention and destruction (e.g., conviction, nonconviction, and juvenile)
   - Who has access to this information for operational and civil purposes?
     - Criminal justice
     - Non-criminal-justice government access
     - Private organizations/individuals
3. Addressing criminal-history data quality and completeness
   - Are required data always collected/submitted?
   - Procedures used by those responsible for these criminal-history record systems to assess information accuracy and completeness (e.g., audits, task force, and financial support)
   - Deficiencies/problems with criminal-history record data (e.g., completeness, accuracy, issues with standardization, delays in updating, and coverage) that are known and what is unknown about the accuracy and completeness
   - Efforts by those responsible for the criminal-history record systems to overcome record system deficiencies (include a few brief examples [perhaps in a box])
   - Additional efforts that others have made to address data deficiencies when using criminal-history records for statistical and research studies
4. How are criminal-history record data used for research purposes?
   - Do government agencies use these criminal justice history data for research purposes? Where available, include examples (e.g., evaluation of interventions)

- What information can be obtained by nongovernmental researchers?
- Procedures to obtain data/access by other government agencies, including typical wait times, institutional review board / approval process, rules on destruction of data
- Procedures to obtain data/access by nongovernment researchers, including typical wait times, institutional review board / approval process, rules on destruction of data
- Ability to link criminal-history data with other data (e.g., mortality/employment info) and discussion of whether these data are available for research versus operational use
- Are some data available to researchers but not law enforcement?

Appendix B. Further Details on Methodology

Below we provide additional information on the two data collection activities undertaken to complement consultations with country experts for Australia, Canada, England and Wales, Germany, and the Netherlands.

Literature and Document Review

The first data collection activity was a review of existing literature and official documentation pertaining to national criminal-history information systems. These sources included academic articles, applicable laws and regulations, government publications, and others (e.g., reports from nongovernmental organizations). In addition to sources recommended by country experts and interviewed key informants, the search strategy for relevant literature was informed by the standardized chapter outline and followed its lines of inquiry. Reflecting the specificities of each national context, no unified formal search strategy was developed. Searches performed by the research team included Google searches, Advanced Google searches, searches of websites of relevant institutions (e.g., national ministries of justice), and searches of repositories of academic literature (e.g., Academic Search Complete and Google Scholar).

Key Informant Interviews

Overview

The second data collection activity was a series of interviews with key informants from the countries. They were either government officials in a position to comment on the country's criminal-history information system (e.g., representatives of agencies managing the national information system and other government agencies, representatives of law enforcement agencies, or staff at government research institutes) or academic researchers who have worked with national criminal-history data.

In total, 39 key informants were interviewed (Table B.1). In some additional instances, country experts offered to consult with colleagues or their national authorities to answer questions raised during the project. Elsewhere, RAND researchers (directly or with the facilitation of country experts) submitted written questions to national authorities responsible for the country's criminal-history information system.

Table B.1. Overview of Interviewees by Stakeholder Group

Stakeholder Group	Count
Representative of a government agency (including entities responsible for the national CRIS)	12
Law enforcement professional	9
Researcher / research manager at a governmental organization	13
Researcher at a nongovernmental organization	5
Total	**39**

Recruitment

The interviewees were identified either through consultations with country experts, desk review, or the research team's professional networks. Potential interviewees were approached via email using standardized invitation language, followed by additional email and phone contact as necessary.

Execution

Interviews were conducted by phone by members of RAND's research team. At the beginning of each session, interviewees were provided with information about the purpose of the interview and how information collected during the conversation would be used. Subsequently, their verbal consent to participate and to be recorded was sought.

While the interviews followed a structure similar to the standardized chapter outline, there was no unified topic guide for the interviews as each discussion was tailored to the specific country context and to address questions raised in the data collection process.

Analysis

Information collected via key informant interviews was incorporated in individual country chapters as appropriate. Given the focus of interviews and the specificities of national contexts, we did not apply any unified analytical framework and did not apply standard qualitative analysis methods. To the extent possible, we examined areas of convergence and divergence across key informant interviews, although the only area of focus that lent itself to this type of analysis was a discussion of data quality and completeness.

AUS Appendix A. Criminal-History Research in New South Wales

AUS A.1 Bureau of Crime Statistics and Research Reoffending Database

The NSW Bureau of Crime Statistics and Research (BOCSAR) is a statistical and research agency that conducts four main strands of activity: it conducts research on crime and criminal justice issues in NSW; it monitors trends in crime and criminal justice; it provides resources and advice to stakeholders on crime and criminal justice; and it maintains statistical databases on crime and criminal justice in NSW. Of most relevance to criminal-history research, BOCSAR maintains the NSW Reoffending Database (ROD), which contains information on every individual who has been convicted of a criminal offense in NSW since 1994. These data are pulled from the local NSW police criminal-history database and contain over 4 million records (with approximately 1.2 million people). Information stored in ROD includes such details as the offender's age, gender, type of offense(s), plea, outcome of court appearance, and penalty. BOCSAR uses its data sets to publish reports summarizing statistical information on recorded crimes and criminal court appearances; to conduct research that evaluates hypotheses and criminal justice interventions; and to provide, on request, statistical information on criminal offenses reported to police and on criminal court appearances to other researchers and members of the public.

ROD assembles data on finalized court matters and police cautions from the NSW police and the NSW court information management system, Justice Link, on a monthly basis. These data, which have not been anonymized, are matched or linked, and additional data files are then added to the records, including mortality records, marriages, police records, and custody records.

External Research Access to Reoffending Database

External researchers may apply for access to the ROD data set via an application form on BOCSAR's website. Applicants must be accredited researchers from an academic or governmental institution and have ethics approval for their research study. Decisions on granting access are made by two senior BOCSAR staff members on an ad hoc basis. The data set will almost always be anonymized when sent externally.

AUS Appendix B. National Criminal Justice Research Agencies

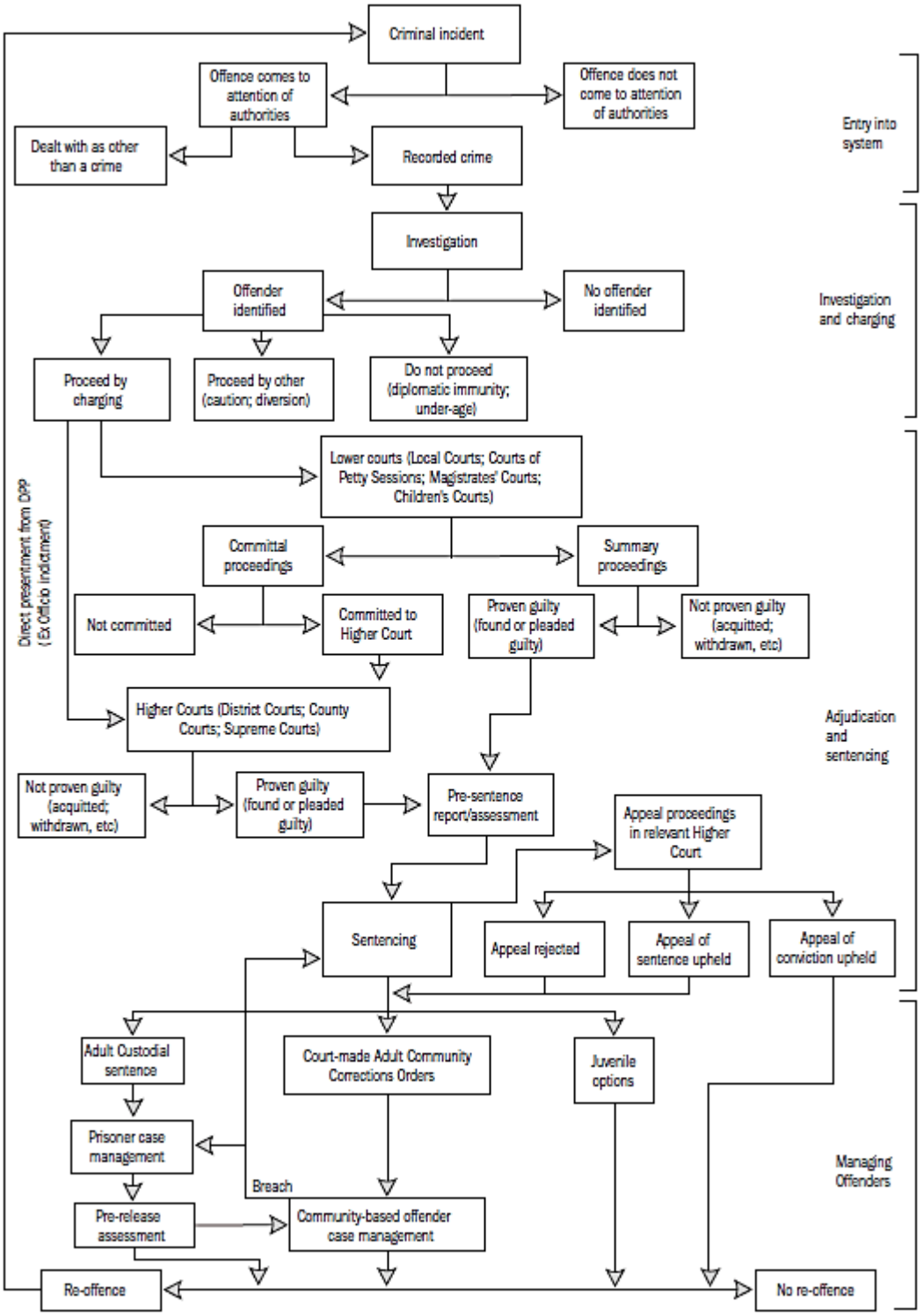
The AIC, established in 1973, is the national research and policy center on crime and justice. AIC research topics currently include child exploitation, cybercrime, deaths in custody, domestic and family violence, homicide, human trafficking and slavery, identity crime, and missing persons. In addition to the research using NPRS data detailed in Section AUS 4, the AIC has a research program called the National Homicide Monitoring Program, which collects and analyzes information from police records, interviews with investigating officers, and coroners' files on all murders and manslaughters (excluding deaths caused by driving) in Australia since 1990. The aim of the project is to identify the characteristics of individuals that place them at risk of homicide and of offending and circumstances that may increase the likelihood of a homicide occurring. The National Armed Robbery Monitoring Program analyzes weapon use in armed robbery and monitors offending trends and patterns, using state and territory police services' armed robbery data on agreed variables.

The Australian Bureau of Statistics (ABS) is Australia's national statistical agency, providing official statistics on crime and justice, among other matters. The ABS coordinates statistical activities and collaborates with state, territory, and Commonwealth agencies in the collection, compilation, and analysis of statistics. In addition, the Australian Bureau of Statistics conducts criminal justice–related surveys, including the Personal Safety Survey and the Crime Victimisation Survey.

AUS Appendix C. Information Flow Through Criminal Justice Systems

The following flow diagram is indicative of the general process of the criminal justice system across Australian jurisdictions. It does not include all complexities or variations of the justice system across jurisdictions.

Figure AUS C.1. Administration of Justice Across Australian Jurisdictions



Source: National Criminal Justice Statistical Framework (4525.0).

E&W Appendix A. Examples of Research Projects Using Police National Computer Data

National Probation Service

An interesting and new use of the PNC data has been implemented by the National Probation Service. The service was set up in 2014 to manage high-risk-of-harm offenders when on conditional release or when serving a community sentence. The remaining probation service (i.e., the management of low-risk-of-harm offenders) was privatized. One role of the National Probation Service is allocating offenders to the high- or low-risk-of-harm categories, and PNC data are used to complete this process. Researchers at HMPPS (which the National Probation Service is part of) built the Risk of Serious Recidivism tool, which analyzes offending history data in the PNC to predict how likely an offender is to commit a seriously harmful offense within two years of release from prison or the commencement of a community sentence. National Probation Service administrators populate the tool with a person's offending history to determine his or her likelihood of a serious offense (Gov.uk, 2019) and then an allocation to high or low risk can be made.

Research Activities

Recidivism / Criminal Career Analyses

Many studies have taken advantage of the data within the PNC. Not all can be reviewed and presented in this chapter, but below are important or interesting current examples that provide a sense of the work completed. Primarily, researchers use the data to understand what drives offending behavior and to describe criminal careers, as well as to evaluate the impact of initiatives designed to reduce reoffending.

Justice Data Lab

The Justice Data Lab was established as a pilot program in April 2013 in response to feedback from organizations working with offenders; these organizations said that they found the process of accessing reoffending data difficult, which, in turn, made it more difficult to evaluate recidivism interventions.[159] The lab provided aggregate reoffending data pertaining to the offenders they had been working with and those of a matched control group. It also provided analyses assessing the statistical significance, if any, of apparent differences in reoffending measures. Initially, the lab provided a one-year proven reoffending rate, but following requests

[159] See MOJ (2015).

from organizations seeking to learn how often people reoffend and the length of time between offending, the lab supplied, in aggregate, the one-year proven reoffending rate, the frequency of proven reoffending over the one-year period, and the time to the first reoffense within the one-year period.[160] The pilot was initially extended for a second year and, in April 2015, was confirmed as a permanent service offered by the MOJ.

The Cambridge Study in Delinquent Development

This study, currently directed by David Farrington, began to follow 411 South London boys in 1961, and subsequently also their children and grandchildren, up to the present day. The original aims of the longitudinal study were "to describe the development of delinquent and criminal behavior in inner-city males, to investigate how far it could be predicted in advance, and to explain why juvenile delinquency began, why it did or did not continue into adult crime, and why adult crime often ended as men reached their twenties" (Farrington, Piquero, and Jennings, 2013, p. 4). The role of the PNC is to provide an accurate conviction history and to validate the interviewees' self-reported convictions. From this information, for example, the study showed that self-reported delinquency had predictive validity (Farrington, 1989).

Police Knowledge Fund

The College of Policing, the Higher Education Funding Council for England (HEFCE), and the Home Office invested £10 million in the Police Knowledge Fund (which began in 2015 and lasted two years). It aimed to increase collaboration between academia and police forces to embed evidence-based policing. Fourteen lead institutions, supported by many more universities and private companies, delivered work ranging from providing courses on police management (University of Cambridge) to restorative justice (University of Sheffield) and an algorithm to predict the likelihood of missing children (University of Nottingham). Many of the projects were dependent on police arrest and conviction data retrieved from the PNC to understand what reduces reoffending and crime.

Cross-Agency Analyses

The MOJ started the Linked Data Project in 2013 to connect convictions histories in PNC data to income and education data to understand offender outcomes across a range of policy areas and the long-term impacts of welfare and education policy options on offending. All offenders over the age of 16 were linked to records about these same individuals in databases held by

[160] A proven reoffense is defined by the Ministry of Justice as "any offence committed in a one-year follow-up period that resulted in a court conviction, or caution in the one-year follow up or a further six-month waiting period (to allow time for cases to progress through the courts)" (MOJ, 2018).

- Her Majesty's Revenue and Customs (to measure income and employment rates)
- Department for Work and Pensions (to measure benefits receipts)
- Department for Business, Innovation and Skills (to measure engagement in further education).

An example analysis from the linked data was a study on the impact of employment on reoffending rates. The authors found that the reoffending rate of offenders who found employment within one year of release from prison was 9.4 percentage points lower than a control group's equivalent rate (MOJ, 2013). Important offending outcome indicators were derived from the linked data set as well. Two years after prison release, 47 percent of offenders were on out-of-work benefits, and 75 percent of offenders made an out-of-work benefits claim at some point. Also, offenders who claimed an unemployment benefit (called a Job Seekers Allowance) spent a longer period on out-of-work benefits than the average claimant (MOJ, 2011).

To Inform/Evaluate Relevant Service Provision

Social Impact Bonds

Social impact bonds (SIBs) are used in the UK to encourage reductions in reoffending. The UK government states

> SIBs improve the social outcomes of public funded services by making funding conditional on achieving results. Investors pay for the project at the start, and then receive payments based on the results achieved by the project. Rather than focusing on inputs (e.g. number of doctors) or outputs (e.g. number of operations), SIBs are based on achieving social "outcomes" (e.g. improved health) (Cabinet Office, 2012).

In the UK, the one outcome paid for through SIBs is a reduction in the proven reoffending rate as measured by PNC data. In fact, the world's first SIB was for a "through-the-gate" intervention at the Peterborough prison in eastern England for prisoners who had served short sentences (less than 12 months). The through-the-gate support involved contacting offenders before release to introduce case workers, assess needs, and plan resettlement activities, which were then completed after release. If the intervention group's frequency of reoffending was 10 percent lower than a control group's rate, extra payments would have been released. The evaluation of the impact was completed using PNC conviction data and unfortunately found a high but not sufficient impact of 8.4 percent (Joliffe and Hedderman, 2014).

Transformation and Rehabilitation

Transforming Rehabilitation is a UK government initiative to focus the probation services in England and Wales on the rehabilitation of offenders and the reduction of reoffending. This included privatizing the management of low- and medium-risk-of-harm offenders, while the management of high-risk offenders remained with the public sector. More importantly for this

discussion, the 21 newly formed Community Rehabilitation Companies are contracted on a payment-by-results basis, whereby their payment is based on their reoffending-rate performance. In other words, if they reduce reoffending as measured in the PNC, they will be paid more by the UK government. Reoffending rates will be compared to a 2011 baseline. If the Community Rehabilitation Company's reoffending rate beats a set confidence threshold, a payment will be released. The reoffending rates are adjusted using the Offender Group Reconviction Scale measure to ensure the current cohort's likelihood to reoffend is similar to the 2011 baseline cohort's likelihood.

One of the Transforming Rehabilitation providers is Sodexo Justice Services, which runs six Community Rehabilitation Companies. Sodexo plans to use PNC data to develop an algorithm to predict the likelihood of reoffending and whether their efforts are reducing the service users' likelihood of reoffending. The algorithm's results will be available in a new offender management system. Why the likelihood has changed and what actions can be taken as a result will be communicated to probation officers to help them deliver effective services. The Police ICT Company, a police force–owned company established to improve police information and communications technology, has made PNC data available through the IDIOM system. In addition to the algorithm, Sodexo plans to use the available PNC data for evaluations to demonstrate the impact of various interventions.

E&W Appendix B. Other Information Systems with Links to the Police National Computer

- **ViSOR.** This is specialist database of detailed records on violent and sexual offenders, used by persons managing such offenders. ViSOR is managed by the National Crime Agency and can be accessed by the police, HMPPS personnel, and private prison companies, enabling them to share risk assessments and risk management information on these offenders through multiagency public protection arrangements. Under the Crime and Courts Act, the length of inclusion in the database depends on the offender's criminal history:
  - indefinitely: imprisonment for 30 months or more, imprisonment for an indefinite period, admission to hospital under restriction order, or subject to an order for lifelong restriction
  - 10 years: imprisonment for 6–30 months
  - 7 years: imprisonment for 6 months or less, or admission to hospital without restriction order
  - 2 years: caution
  - conditional discharge: period of discharge or probation
  - any other: 5 years.

  If the person is under 18 years of age when convicted or cautioned, finite notification periods are halved. Offenders may appeal against indefinite inclusion to the local police force after 15 years. A recent pilot was completed to automatically update the offender manager, via ViSOR, when an arrest or conviction record was entered on the PNC.
- **Police National Database (PND).** A national "soft intelligence" handling system that contains all the information stored in PNC, as well as operational policing information and details of allegations and/or investigations that did not result in an arrest. This intelligence is input by individual police forces and may be accessed only by law enforcement officers.
- **National Firearms Licensing Management System.** Firearm certificate holders are marked on the PNC, and it automatically notifies all police forces of changes to a certificate holder's personal record on the PNC. This includes arrests and convictions.
- **IDIOM.** A web-based offender tracking tool to manage high-risk or high-harm offenders in the community. It is provided to police forces by the Home Office to support Integrated Offender Management arrangements, an initiative in England and Wales aimed at enabling all relevant criminal justice agencies to coordinate offender management. Individuals subject to Integrated Offender Management arrangements are marked manually on the PNC, and an overnight feed of arrests and updated outcomes is added to IDIOM from the PNC.

DEU Appendix A. Comparison of National-Level Information Systems in Germany

Table DEU A.1 below presents an overview of national-level information systems collecting data on persons who come in contact with the criminal justice system in Germany. As the main national repository of criminal-history information, the BZR is discussed in the main body of this appendix. ZStV and BKA files are discussed in Appendixes B and C.

Table DEU A.1. Overview of National-Level Information Systems in Germany

System	BZR	ZStV	BKA Files
Purpose	Repository of criminal records	Coordination of criminal investigations	Support to criminal investigations
Contents	Court convictions (and public prosecutor and court disposals of juvenile cases)	Information pertaining to criminal investigations	Information pertaining to criminal investigations
Governed by	BZRG	StPO[a]	Bundeskriminalamtgesetz (BKAG)
Managed by	BfJ	BfJ[b]	BKA[c]
Data provided by	Courts and other reporting authorities	Public prosecutor offices	Law enforcement agencies
Accessible by	Selected public institutions, individuals, researchers, and employers[d]	Agencies involved in criminal investigations	Agencies involved in criminal investigations

[a] The system's operation is further guided by a specific regulation (Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters).
[b] The BfJ provides only hardware and administrative support. Ownership of data and responsibility for their quality rests with contributing agencies.
[c] Ownership of data and responsibility for their quality rests with contributing agencies (other than the BKA).
[d] Individuals have access only to their own records. A certificate of conduct applied for by the individual concerned (typically for employment purposes) can then be provided to employers.

DEU Appendix B. Zentrales Staatsanwaltliches Verfahrensregister

DEU B.1 History and Organizational Management

In addition to the BZR, another existing system with information on individuals involved in the criminal justice system is the central register of criminal proceedings, the ZStV.[161] It is also known as the prosecutors' information system, or SISY (Staatsanwaltliches Informationssystem). However, unlike the BZR, the ZStV serves only prosecution purposes. It facilitates the coordination of investigations led by different public prosecution offices that may involve the same individuals and avoid any double prosecution.

The ZStV was established in 1999 and, as with the BZR, is administered by the BfJ. Sections 492–495 of the StPO are the underlying legal basis, and the system's operation is further guided by a specific regulation (Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters). The system receives approximately 30,000 daily information requests, and the BfJ estimates the volume of data at 30 million entries.[162]

DEU B.2 Content

The ZStV holds data pertaining to criminal proceedings in Germany independent of police data records. Its records consist of the following:

- personal information: name, date and place of birth, sex, citizenship, address, and physical marks, such as scars and tattoos
- custody-related information (where applicable)
- offense data: place and time of offense, applicable statute, description of the offense, monetary damage, and information on co-suspects
- operational and procedural data pertaining to the investigation of the offense
- final decisions of prosecution authorities or courts (acquittals and dismissals).

Public prosecutors and finance authorities responsible for prosecuting tax evasion have an obligation to report information to the ZStV. The information must be provided as soon as the authorities begin their investigation. (Usually this is the case when police have passed the file on

[161] In addition to expert input and applicable legislation, sources relevant for this section include Satzger, Schluckebier, and Widmaier (2016), Topfer (2009), and Deutscher Bundestag (2009).

[162] This estimate is based on the approximately 6 million records created annually multiplied by an approximate average length of data retention of five years (BfJ, n.d.c).

to the public prosecutor.) Data reported must be transferred electronically in a unified form via the automatic reporting and information procedure.

DEU B.3 Data Quality

There is no central system for auditing the quality and accuracy of data held in the ZStV. Unlike the BZR, the role of the BfJ in overseeing the database is limited to the provision of hardware and administrative support. Data held in the ZStV are not owned by the BfJ and belong to the contributing prosecution offices. Therefore, data quality depends on the processes of the contributing agencies.

DEU B.4 Data Retention

According to Section 494 of the StPO, entries in ZStV must be erased if they

- are proven wrong or as soon as the conviction of the defendant has become valid
- must be recorded in the Central Register via a separate procedure according to the BZRG.

There is no legal provision for a connection between the ZStV (populated based on prosecutor files) and the BZR (populated based on court files). Therefore, data are not transferred from one database to the other. Ultimately, conviction data will be recorded only in the BZR and cannot be double registered simultaneously in the ZStV. Entries also must be deleted when the defendant has been acquitted or the proceedings are ended by a final decision of prosecution authorities or courts, especially by dismissals. In these cases, the information will be kept for up to two years and subsequently deleted, provided there is no new offense registered by the same person during these two years.

DEU B.5 Access to Data

Information from the ZStV may be given only to criminal law enforcement authorities (including police) for the purpose of criminal investigative proceedings. This includes tax authorities involved in criminal investigations and tax and customs authorities but not administrative agencies and courts. In addition, Section 492 of the StPO gives restricted access to ZStV data to the three German secret services (foreign intelligence, Bundesnachrichtendienst; domestic intelligence, Bundesamt für Verfassungsschutz; and military intelligence, Militärischer Abschirmdienst).

In addition to German criminal law enforcement authorities, data can be shared with national members of Eurojust (the EU agency for judicial cooperation), which includes all 28 EU member states. Other authorities, private entities, and researchers have no access to the ZStV.

Individuals can request to review information that is held on them in the ZStV. Before providing this information, the BfJ has to get the prosecutor's agreement to avoid jeopardizing the ongoing investigation.

DEU Appendix C. Bundeskriminalamt Data

DEU C.1 History and Organizational Management

BKA databases are operated by the BKA in accordance with the BKAG.[163] The central police information system (INPOL) was established in 1972 and updated in 2003 (INPOL-neu). The AFIS was established in 1993, and the DNA database was established in 1998. As of 2017, the BKA held approximately 3.6 million items of personal data.[164]

DEU C.2 Content

As defined by Section 8 of the BKAG, the BKA is allowed to gather and keep only information on offenses and related suspicions, such as data related to ongoing investigations. Specifically, the BKA is allowed to collect the following:

- personal identification data on the accused person
- information pertaining to the alleged offense
- information about the agency involved in the investigation and record number.

BKA databases fall into three categories:

- **Joint files** (*Verbunddateien*). Managed by the BKA but automatically populated with data from contributing agencies, which include the 16 German state police forces, the federal police, and the customs service and its criminal investigation branch. Data from these files are shared via the central interface INPOL. INPOL data are organized in two types of files: personal and property.
- **Central files** (*Zentraldateien*). Populated by the BKA based on information shared by partner agencies (e.g., secret services). They are available for read-only access to other users.
- **Office files** (*Amtsdateien*). Contain internal information for the BKA, operated and accessed exclusively by the BKA.

BKA data files include several databases. Examples containing biometric information (although with no possibility to link with the BZR) include

- **AFIS.** A database of fingerprint sheets made during police identification measures. As of January 2018, it contained fingerprints for approximately 2.8 million persons and palmprints for approximately 1.9 million persons.[165]

[163] In addition to expert input and applicable legislation, sources relevant for this section include Topfer (2009) and Deutscher Bundestag (2009).

[164] See BKA (n.d.c).

[165] See BKA (n.d.b).

- **DNA database.** Collects data from accused and convicted persons and prints from crime scenes. As of 2017, it contained almost 1.2 million data records.[166]

DEU C.3 Data Collection and Storage Rules

As mentioned above, data held by the BKA must be related to actual investigations and should be deleted once the investigation is over. Some data can be stored in special databases (e.g., the DNA database) for the purpose of future criminal investigation, and police are allowed to check whether a suspect in a current investigation has a former entry in such a database. With respect to data provided by state police agencies, data collection and storage arrangements are governed by the police laws of the 16 federal states (i.e., applicable rules depend on the origin of the information in question). However, these state laws are all similar, building on a template provided by a federal model police law. For personal data obtained in the context of border crossing, data collection and storage are governed by Section 29 of the Bundespolizeigesetz (Federal Police Act) (Bundesministeriums der Justiz und für Verbraucherschutz, 2017a).

DEU C.4 Access to Bundeskriminalamt Data

With few exceptions, access to BKA databases is limited to police authorities, which have the ability to transfer data within Germany and to other EU police authorities and Europol. BKA files are linked to existing European systems:

- AFIS contributes to Eurodac (European database of fingerprint information).
- The DNA database is linked with similar systems in other countries under the Prüm System (an EU data-sharing system of DNA information).
- The BKA is Germany's national point of contact for the Schengen Information System (a law enforcement information system supporting the European border-free travel zone).

The BKA itself carries out research based on individual-level data if anonymized, or it can commission researchers to conduct certain research projects (§29 BKAG). Aggregate statistical data are made available annually by the BKA in the Police Crime Statistics (Polizeiliche Kriminalstatistik).

[166] See BKA (n.d.a).

NLD Appendix A. Police Databases

NLD A.1 Content

Before 2009, different police units used different data systems to capture information on crimes and suspects. Since then, however, each regional unit of the Dutch police captures this information in a standardized data system called the Primary Information Provision for Law Enforcement (Basisvoorziening Handhaving [BVH]). Data are entered into the BVH manually by originating agencies. Information captured in the system includes

- a description of the nature of the offense
- the standardized incident code of the offense (in line with the Statistics Netherlands incident code)
- details on the suspect
- location of the offense
- information on individual reporting the offense (Criminaliteit in Beeld, 2018).

In addition, the JDS provides information on court dispositions to police agencies and their staff and then enters the data into BVH.

Most of the information captured in the BVH feeds into a central data warehouse called the Primary Information Provision Database (BVI). Each regional unit provides the Police Service Centre with most information as held in the BVH. The Police Service Centre in turn adds this information from all regional units to the national-level BVI. This reporting process from the BVH to the BVI repository is automated. In addition to law enforcement data captured by the BVH, the BVI retrieves data on criminal investigations through the Summ-IT system (Algemene Rekenkamer, 2016). This system, also populated by police officers, supports ongoing criminal investigations (Flex-I.D., 2018).

This structure of the BVH and Summ-IT has been in place for several years, and its development is part of a long-term process of improving the data infrastructure of the police, which is aimed at culminating in the development of a single, integrated information and communication technology system of the operational police work (Algemene Rekenkamer, 2016; Politie, 2017).

NLD A.2 Access to and Use of Police Databases for Operational Purposes

The BVI is the main interface to consult police data for operational purposes. It enables authorized users to query the system and extract resulting information reports. Data held in the BVI are used for ad hoc information requests and ongoing investigations by police officers. In addition, crime data are used to inform police strategies, for example, through highlighting high-impact crimes and detailed crime analyses.

NLD A.3 Access to and Use of Police Databases for Research Purposes

Procedures to Access Police Data for Research Purposes

Providing access to police databases for most purposes falls under the responsibility of the Bureau for Management Information of the National Police Leadership Team (Bureau Management Informatie). In general, the access procedure consists of the following steps:

1. The prosecutor general (*parket generaal*) approves external requests for access to police data.
2. The Knowledge & Information Team (Kennis en Informatie) then assesses the relevance of the request.
3. The Bureau of Management Information then assigns the parties requesting the data to relevant people in the police organization (depending on the research topic) and discusses the feasibility of obtaining the data.
4. The police have special arrangements with some external parties, such as Statistics Netherlands and the WODC, to share police data on a regular basis.

In general, only Statistics Netherlands receives identifiable data from the police database in order to enable data linkage. Statistics Netherlands subsequently anonymizes the data by transferring it into a unique code. They are obliged to destroy raw data as soon as research is completed. Secured data (i.e., after anonymization) can be stored for longer periods if it is used for research purposes.

When requesting access to police data for research purposes, researchers should have the relevant security clearances, such as a certificate of conduct (*verklaring omtrent gedrag*). Permission to use police data will not be granted for studies looking at groups of fewer than ten individuals. Personal identifiers will generally not be included in the database unless there is a specific request or when it involves annual data provision to Statistics Netherlands, as described above. Another way for scientific researchers to gain access to police data is requesting such data via Statistics Netherlands.

There are three ways in which data can be accessed. First, researchers can access microdata via Statistics Netherlands' stand-alone computers based at various locations in the Netherlands. The identity of the researcher is checked through a fingerprint-recognition system. Second, researchers can gain access to microdata at Statistics Netherlands' headquarters. For both options, researchers are not permitted to retain raw data or outputs from statistical software, such as IBM's SPSS software, and any output analyses stemming from these data are checked by Statistics Netherlands. Finally, in some cases, Statistics Netherlands conducts analyses of the data on researchers' requests.

Possibilities and Limitations of the Use of Police Data for Research Purposes

Police databases in the Netherlands are accessible for multiple research purposes:

- scientific research into, for example, crime rates and criminal careers[167]
- informing the Dutch House of Representatives on specific topics
- responding to freedom-of-information and media requests
- calculating capacity for the agencies involved in the criminal justice system
- examining how cases flow through the criminal justice system, for example, from arrest to execution of sentence.[168]

Data Linkage Using Police Data

Statistics Netherlands is the main authority in the Netherlands responsible for linkage between police data and other information, such as demographics. They receive raw, identifiable data from the national police system, the BVI, on an annual basis and subsequently anonymize the data by transferring it into a unique code. The raw data include the individual's identifying BSN. Since 2007, every individual who is registered in the BRP—which includes details on those living in and outside of the Netherlands—automatically receives a BSN (Government of the Netherlands, n.d.b, n.d.e).[169] This number "is a unique personal number allocated to everyone registered in the Municipal Personal Records Database [and] is recorded on [an individual's] passport, driving license and identity card" (Government of the Netherlands, n.d.e). Different authorities in the Netherlands work with these personal numbers, such as the tax department and health services (Government of the Netherlands, 2013). As such, the BSN is a crucial item for making linkages to other (demographic) data.[170] One interviewee also recognized that the BSN is increasingly used to link data but added that there are still cases in which data linkage is not as straightforward. For example, some databases use BSN, while others use identifiers as used by municipalities (Gemeentelijke Basis Administratie) or numbers as used in court.

After anonymization, the newly created unique code is used by Statistics Netherlands for linkage to other databases, and any data sets shared with other researchers include this anonymized identification number. As Statistics Netherlands has the original, identifiable BSN numbers, they are exclusively placed to link the data with, for example, demographics.

---

[167] This could also involve linking offender data to demographics (e.g., age, gender, and ethnicity). Police databases do have information on criminal history like the OBJD, but the police databases also include information on cases that did not result in a conviction, which could be problematic when making statements about criminal careers based on proven offending. That said, there are options for researchers to receive police data that are cleaned and include only cases that went to the prosecution stage.

[168] Administrative data from police and other agencies in the criminal justice system are analyzed by the Criminal Justice System Directorate (Directie Strafrechtsketen).

[169] The introduction of BSN replaced the so-called *sofinummer*, which was used before 2007 for similar purposes. According to Government of the Netherlands (n.d.d), "Municipalities record the personal data of all residents in BRP. These data include marriage, the birth of a child, or a change of address. If someone moves to another municipality, their personal data moves with them."

[170] Statistics Netherlands also maintains a separate database for individuals without a registration number (e.g., undocumented migrants), although this data set is less reliable. Registration practices were digitalized in the mid-1990s, and as such, Statistics Netherlands is not able to make linkages for earlier years.

NLD A.4 Data Quality and Completeness

Issues around quality and completeness of police data range from the broader issue of crimes not recorded by the police to inconsistent recording by police officers at the local level. Box 3 below outlines the key issues as reported by interviewees.

Box 3. Quality and Completeness of Dutch Police Data

- **Dark number.** Crimes that are not reported to or identified by the police do not show up in police databases.
- **Inconsistent recording practices.** The recording of crime is inconsistent across different police forces. For example, while some forces capture several crimes committed by one person under one file, others record these cases separately. When using these data for research projects, researchers address this issue by reporting on whether someone was suspected of a crime, instead of looking at the number of crimes per individual.
- **Incorrect or incomplete reporting/recording practices.** The location where crimes were committed is not always recorded correctly. For example, when an offense took place during a train journey, it is not always possible to determine the precise location of the offense. A correct address is recorded for around 70 percent of the offenses included in police databases. Also, not all details of an offense are included in the central BVI police data system as police reports are not transferred over from the local BVH database.
- **Classification of crimes.** For some offenses, such as domestic violence, there are currently no specific incident codes. As a result, several crimes could fall under one code (e.g., domestic violence classified as a violent incident). This could affect how data can be used for operational and research purposes.
- **Limited details.** Police data do not capture much of the detail that would be beneficial for research purposes. For example, for some offenses (such as sex offenses), additional details are not recorded in police databases (such as age and gender of victims).
- **Information on dismissals.** The central police database does not show what cases were dismissed. Statistics Netherlands is currently trying to establish a link with OM data to address this issue.
- **Historical patterns.** Since the police database as used for research purposes was established in the mid-1990s, researchers aiming to map criminal careers can study historical patterns only from that period onward.

NLD A.5 Procedures to Address Deficiencies

In addressing data quality issues, according to the Dutch police, the introduction of the national police database, the BVI, has resulted in several improvements (Criminaliteit in Beeld, 2018), including the following:

- The completeness and comparability of data at the regional level due to a standardized reporting format have increased.
- Double registering and double counting crimes has been prevented. Crimes are registered only in the region where they were committed. (Previously, crimes were counted in both the region where they were reported and where they took place.)
- The mutual comparability of data held by police and by Statistics Netherlands has improved. (Previously, Statistics Netherlands did not use the same counting method as the one used for police databases.)
- The classification of crimes by main categories and subcategories has been improved, expanded, and standardized.

In another ongoing effort, the Dutch police are working on improving the process of inputting data on court dispositions received from the JDS, which is currently done manually

and prone to errors. Data input involves both automatic and manual processes through specialized departments.

In the event of data requests by third parties, the Bureau of Management Information conducts checks on the validity of police data requested. While the Bureau of Management Information cannot make changes to the original police database, it can make changes to the extracted data and/or inform parties requesting the data about these omissions in the data or changes that were made.

Statistics Netherlands also conducts checks on the data, including plausibility checks, imputation of missing data, and comparisons of outputs with previous trends to spot possible major outliers. As mentioned above, the Bureau of Management Information informs Statistics Netherlands in advance about changes made to the data set, such as the addition of new incident codes, which then helps to explain (new) crime trends where this is the case. As pointed out by an interviewee, the reliability of the data differs per source. The interviewee suggested that individual-level data on suspects are correct in 90–95 percent of the cases, with missing data including details on foreign tourists for which personal data are not known. Police data on suspects is generally more reliable than information on victims as the police tend to record suspect details better for investigation purposes. When linking police data with other data, such as demographics, a team at Statistics Netherlands conducts reliability checks based on different items, such as BSN, sex, and date of birth. This team subsequently reports to the relevant team what data are most reliable to use.

NLD Appendix B. Further Details on Access to Judicial Document System Data

As discussed in Section NLD 2.4, a variety of persons, institutions, and organizations can be granted access to JDS data. The Judicial Data Act establishes a range of purposes for which data can be accessed and describes which entities may access judicial data for each purpose. The circumstances of data access (including type of data, purpose of data access, preconditions of access, data retention, and sharing with third parties) are governed by a diverse and detailed body of rules. These rules are not limited to the Judicial Data Act alone and are frequently documented in secondary legislation referred to in the Judicial Data Act.

Table NLD B.1 below presents a nonexhaustive overview of entities that are authorized to access criminal and judicial data. The table is structured along the lines of the broad groups of information objectives listed in Section NLD 2.4 and broadly corresponding to the individual sections of Chapter 3 of the Judicial Data Act.[171] The first objective deals with the provision of certain data to (a) execute a task, (b) provide advice, and (c) make administrative decisions. Under this information objective, entities are allowed to access data only on convictions where the person concerned received an unconditional sentence, typically limited to four years after the sentence has expired.[172] The second objective refers to the provision of data in a general sense for (a) the execution of a task, (b) the hiring and dismissal of personnel, and (c) the provision of advice, recommendation, or nomination of persons. Data in a general sense cover all available data on criminal cases within the standard retention periods for each type of offense (see Table 6.1) (Helsloot et al., 2013).

Table NLD B.1. Dutch Judicial Data Act—Provision of Data on Judicial and Criminal Proceedings

Purpose		Examples of Authorities with Access to Judicial Data in Certain Circumstances[a]
1) Provision of certain data	a. Execution of task	• Chair of the Commission Violent Offenses Compensation Fund (Art. 11) • Mayor or municipal executive or by a civil servant appointed by the mayor or municipal executive (Art. 11a, 11c) • Commissioner of police (Art. 11b) • The Board of Procurators General (OM's highest authority; oversees internal investigations) (Art. 11b) • Minister of defense (Art. 11b) • Minister of finance (Art. 11b) • Minister of housing, spatial planning, and the environment (Art. 11b)

[171] Chapter 3 of the Judicial Data Act also includes provisions of data for research purposes. This topic is addressed in Section NLD 4.

[172] This period is extended for information for more severe sentences. Additional restrictions apply with respect to data on youth persons.

		• Minister of agriculture, nature, and food quality (Art. 11b) • Minister of social affairs and employment (Art. 11b) • Legal Aid Board (Art. 11d)
	b. Provision of advice	• The Minister of justice (Art. 12) • Mayors (Art. 12)
	c. Administrative decisions	• Persons or boards tasked with taking decisions as defined under the General Administrative Law Act regarding the laws as listed in the article (e.g., Licensing and Catering Act) or those handling the appeal of these decisions (Art. 13) • Administrative bodies tasked with taking decisions regarding the imposition of administrative fines by one of the laws listed in the article (e.g., Unemployment Insurance Act) (Art. 13a)
2) Provision of data in a general sense	a. Execution of task	• The head of General Intelligence and the Security Service (Art. 14) • The head of Military Intelligence and the Security Service (Art. 14) • National Public Administration Probity Screening Act Bureau (performs integrity screenings as requested by public administration bodies as set out in the Public Administration Probity Screening Act) and the legal persons performing government tasks that make successful requests to the bureau (Art. 15) • Administrative bodies taking decision regarding the implementation of provisions in the Temporary Law on Counterterrorism Administrative Measures (Art. 15a) • Minister of justice (Art. 16) • Mayors (Art. 16) • Commissioner of police (Art. 16, 21) • Minister of defense (Art. 16) • Directors of rehabilitation and penal institutions (Art.17, 18) • Probation officers (Art.17) • Juvenile rehabilitation personnel (Art.17) • Director of the Children and Family Court Advisory and Support Service or his or her substitute (Art.17) • Behavioral experts (Art.17) • Forensic care providers (Art.17) • Council for the Administration of Criminal Justice and Protection of Juveniles (advises the minister and the state secretary of justice and security and the state secretary for health, welfare, and sport and acts as a court of appeal for decisions regarding prisoners or persons serving a custodial measure) (Art.18a) • Minister of immigration, integration, and asylum (Art. 19) • All parties charged with supervising and enforcement of the Schengen Borders Code, statutory regulations regarding aliens and their sponsors (Art. 19) • The authorities tasked with implementing the Passport Act (Art. 20) • The acting public prosecutor (Art. 21) • The head of the service in charge of dealing with requests for legal assistance within the National Unit of the police force (Art. 21) • The commander of the Royal Netherlands Marechaussee (the gendarmerie, a police force with military status) (Art. 21) • The head of the Financial Intelligence Unit (Art. 21) • Minister of infrastructure and environment (minister of justice acts as an intermediary) (Art. 22a) • Minister of social affairs and employment (minister of justice acts as an intermediary) (Art. 22c) • Municipal executive (minister of justice acts as an intermediary) (Art. 22c)
	b. Hiring and dismissal of personnel	• The head of General Intelligence and the Security Service (Art. 23) • Commissioner of police (Art. 23) • Minister of justice (Art. 23, 24)

		• The Board of Procurators General (OM's highest authority; oversees internal investigations) (Art. 23) • Minister of foreign affairs (Art. 23) • Director general of the Tax Administration (Art. 23) • The contact officer for queries pertaining to the General Tax Act (Art. 23) • Staff of the fraud team, the authorization manager, and application manager (Art. 23) • Head of the management team of the Tax Administration / the Netherlands Fiscal Intelligence and Investigation Service (Art. 23) • Head of the General Inspection Services reporting to the Ministry of Economic Affairs, Agriculture, and Innovation[b] (Art. 23) • Inspector general of the Transport and Water Management Inspectorate (Art. 23) • Directors of penal institutions (Art. 23, 25) • Directors of institutions that care for those detained under hospital order (Art. 23, 25) • Directors of institutions temporarily dealing with persons in custody or convicted under the Opium Act (Art. 23, 25) • Directors of those (parts of) penitentiaries that hold foreign nationals detained under the Aliens Act (Art. 23, 25) • Directors of a youth detention center (Art. 23, 25) • Euroclear Nederland (Central Institute for Securities Transactions) (Art. 26) • President of the Dutch central bank • President of Joh. Enschedé Facilities BV (a company specialized in printing banknotes, security documents, and stamps) (Art. 26) • Chair of the Netherlands Authority for the Financial Markets (Art. 26) • Head of Company Security Services at KLM (Art. 27) • Director of SAGEM Identification BV, a subsidiary of Morpho (a company producing biometric identity documents) (Art. 27)
	c. Advice, recommendation, or nomination of persons	• The chair of the commissions tasked with selecting future employees with the judiciary or OM (Art. 29) • The persons in charge of drawing up a recommendation for the occupation of the office of the national ombudsman or substitute ombudsman (Art. 29) • The chairs of oversight boards (Art. 29) • Commissioner of police (Art. 29) • Secretary-general to the minister of justice and security (Art. 30) • Minister of the interior and kingdom relations (Art. 30) • The queen's commissioners (head of a province)[c] (Art. 30) • Mayors (Art. 30) • The kingdom representative at public bodies of Bonaire, St. Eustatius, and Saba (Art. 30) • Minister of defense (Art. 30)
3) Provision of data to partners abroad		• Competent authority of a foreign country (Art. 32, 33) • The central authority of another EU member state (Art. 34, 35, 36, 37) • Eurojust (Art. 41) • Europol (Art. 42) • National liaison officers at Europol (Art. 42)

[a] These circumstances, as well as what specific data can be requested, are specified in the corresponding sections of the Judicial Data Act.
[b] This Ministry was a fusion of the Ministry of Economic Affairs and the Ministry of Agriculture, Nature, and Food Quality from 2010 until 2017, when they were split again. The former became the Ministry of Economic Affairs and the Environment.
[c] Since the queen's abdication in 2013, these are now the king's commissioners.

References

ABS—*See* Australian Bureau of Statistics.

ACRO—*See* Association of Chief Police Officers Criminal Records Office.

Adams, E. B., E. Y. Chen, and R. Chapman, "Erasing the Mark of a Criminal Past: Ex-Offenders' Expectations and Experiences with Record Clearance," *Punishment and Society*, Vol. 19, No. 1, 2017, pp. 23–52.

Aebi, M. F., M. M. Tiago, and C. Burkhardt, *SPACE I—Council of Europe Annual Penal Statistics: Prison Populations: Survey 2015*, updated on April 25, 2017, Strasbourg: Council of Europe.

Alain, M., R. R. Corrado, and S. Reid, *Implementing and Working with the Youth Criminal Justice Act Across Canada*, Toronto: University of Toronto Press, 2016.

Alberta Justice and Solicitor General, "Criminal Prosecutions," n.d. As of October 11, 2018: https://justice.alberta.ca/programs_services/criminal_pros/Pages/default.aspx

Algemene Rekenkamer, "ICT politie 2016: Vervolgonderzoek naar de ICT-governance en de basisvoorzieningen voor handhaving en opsporing bij de nationale politie," The Hague: Algemene Rekenkamer, 2016.

Allen, M., "Police-Reported Crime Statistics in Canada, 2017," Statistics Canada, July 23, 2018. As of October 11, 2018: https://www150.statcan.gc.ca/n1/pub/85-002-x/2018001/article/54974-eng.htm

Association of Chief Police Officers Criminal Records Office, "Retention Schedule," n.d. As of June 10, 2019: https://www.acro.police.uk/acro_std.aspx?id=697

Australian Bureau of Statistics, "4513.0—Criminal Courts, Australia, 2016–17," February 28, 2018. As of February 13, 2019: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/4513.0~2016-17~Main%20Features~All%20Courts~5

———, "Recorded Crime—Offenders, 2017–18," March 15, 2019a. As of June 10, 2019: https://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/4519.02017-18?OpenDocument

———, "Corrective Services, Australia, March Quarter 2019," June 6, 2019b. As of June 10, 2019: https://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/4512.0March%20quarter%202019?OpenDocument

———, “Australian Demographic Statistics, Sep 2018,” June 20, 2019c. As of August 7, 2019: https://www.abs.gov.au/AUSSTATS/abs@.nsf/mf/3101.0

Beard, J., *The Retention and Disclosure of Criminal Records*, House of Commons Library, Briefing Paper CBP6441, May 17, 2019. As of June 10, 2019: https://researchbriefings.files.parliament.uk/documents/SN06441/SN06441.pdf

BfJ—*See* Bundesamt für Justiz.

Bibel, D., “The Quality of Official Crime Data,” *Conference Papers—American Society of Criminology*, American Society of Criminology Annual Meeting, Atlanta, November 2007, p. 1.

BKA—*See* Bundeskriminalamt.

Boogaard, G., and J. Uzman, “Artikel 122—Gratie,” Nederland Rechtsstaat, 2019. As of August 21, 2019: https://www.nederlandrechtsstaat.nl/grondwet/artikel.html?artikel=122&categorie=&auteur=&trefwoord=&1=1##artikel122

British Columbia Civil Liberties Association, “Canadian Police Information Centre (CPIC),” 2015. As of October 11, 2018: https://bccla.org/privacy-handbook/main-menu/privacy7contents/privacy7-14.html

Bundesamt für Justiz, “Anfragen und Mitteilungen zur Registerbehörde per elektronischer Datenübermittlung,” n.d.a. As of August 13, 2019: https://www.bundesjustizamt.de/DE/Themen/Gerichte_Behoerden/Register/Datenuebermittlung/Datenuebermittlung_node.html

———, “Welcome to the Federal Office of Justice,” n.d.b. As of July 1, 2019: https://www.bundesjustizamt.de/EN/Home/homepage_node.html

———, “Zentrales Staatsanwaltschaftliches Verfahrensregister (ZStV),” n.d.c. As of August 13, 2019: https://www.bundesjustizamt.de/DE/Themen/Gerichte_Behoerden/ZStV/ZStV_node.html

———, “10 Jahre Bundesamt für Justiz,” 2017. As of August 13, 2019: https://www.bundesjustizamt.de/DE/Presse/Archiv/2017/20170323.html?nn=3451904

Bundeskriminalamt, “DNA-Treffer Statistik,” n.d.a. As of August 13, 2019: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/DNA-Analyse/DNAstatistik/dnaStatistik_node.html

———, “Fakten und Zahlen zu AFIS,” n.d.b. As of August 13, 2019: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/AFIS/afis_node.html

———, “Sammlung, Auswertung und Steuerung von Informationen,” n.d.c. As of August 13, 2019: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/SammlungAuswertungSteuerung/sammlungauswertungsteuerung_node.html

———, “Polizeiliche Kriminalstatistik,” 2019. As of June 10, 2019: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2018/pks2018_node.html

Bundesministeriums der Justiz und für Verbraucherschutz, Bundespolizeigesetz [Federal Police Act], May 2017a. As of August 13, 2019: https://www.gesetze-im-internet.de/bgsg_1994/BJNR297900994.html

———, Bundeskriminalamtgesetz [Federal Criminal Police Act], June 2017b. As of August 13, 2019: https://www.gesetze-im-internet.de/bkag_2018/BKAG.pdf

———, Personenstandsgesetz [Civil Status Act], December 2018. As of August 14, 2019: https://www.gesetze-im-internet.de/pstg/BJNR012210007.html

———, Bundeszentralregistergesetz [Federal Central Criminal Register Act], June 2019a. As of August 13, 2019: http://www.gesetze-im-internet.de/bzrg/

———, Jugendgerichtgesetz [Act on Juvenile Courts], June 2019b. As of August 13, 2019: http://www.gesetze-im-internet.de/jgg/index.html

———, Strafgesetzbuch [Criminal Code], June 2019c. As of August 14, 2019: https://www.gesetze-im-internet.de/stgb/

———, Strafprozessordnung [Rules of Criminal Procedure], July 2019d. As of August 14, 2019: https://www.gesetze-im-internet.de/stpo/index.html

Bureau, B., “RCMP Database Remains out of Date, Police and Prosecutors Say,” CBC News, March 10, 2015. As of October 11, 2018: https://www.cbc.ca/news/politics/rcmp-database-remains-out-of-date-police-and-prosecutors-say-1.2989397

Cameron, D., and R. Simeon, “Intergovernmental Relations in Canada: The Emergence of Collaborative Federalism,” *Publius: The Journal of Federalism*, Vol. 32, No. 2, 2002, pp. 49–72.

Canadian Civil Liberties Association, *Non-conviction Records*, May 2014. As of October 11, 2018: http://www.ccla.org/recordchecks/doc/Non-Conviction%20Records.pdf

Canadian Society for Evidence-Based Policing, “Good Data Initiative,” n.d. As of October 11, 2018: http://www.can-sebp.net/good-data-initiative

CAN-SEBP—*See* Canadian Society for Evidence-Based Policing.

CBS—*See* Centraal Bureau voor de Statistiek.

CCLA—*See* Canadian Civil Liberties Association.

Centraal Bureau voor de Statistiek, "Gedetineerden; geslacht, leeftijd en herkomstgroepering," 2017. As of October 29, 2018: http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=82321ned.

———, "Bevolkingsteller," 2018a. As of October 29, 2018: https://www.cbs.nl/nl-nl/visualisaties/bevolkingsteller

———, "Gemeentelijke indeling op 1 januari 2018," 2018b. As of October 29, 2018: https://www.cbs.nl/nl-nl/onze-diensten/methoden/classificaties/overig/gemeentelijke-indelingen-per-jaar/indeling%20per%20jaar/gemeentelijke-indeling-op-1-januari-2018

Conor, P., "Police Resources in Canada, 2017," Statistics Canada, March 28, 2018. As of October 11, 2018: https://www150.statcan.gc.ca/n1/pub/85-002-x/2018001/article/54912-eng.htm

Corda, A., "Beyond Totem and Taboo: Toward a Narrowing of American Criminal Record Exceptionalism," *Federal Sentencing Reporter*, Vol. 30, No. 4–5, 2018, pp. 241–251.

Correctional Service Canada, "Our Role," 2016. As of October 11, 2018: http://www.csc-scc.gc.ca/about-us/006-0001-eng.shtml

Council of the European Union, "Council Decision 2009/316/JHA of 6 April 2009 on the Establishment of the European Criminal Records Information System (ECRIS) in Application of Article 11 of Framework Decision 2009/315/JHA," *Official Journal of the European Union*, April 7, 2009.

Courts and Tribunals Judiciary, "Magistrates' Court," n.d. As of June 10, 2019: https://www.judiciary.uk/you-and-the-judiciary/going-to-court/magistrates-court/

Court Statistics Project, "Total Incoming Criminal Caseloads Reported by State Courts, All States, 2007–2016," 2018. As of February 13, 2019: http://www.courtstatistics.org/~/media/Microsites/Files/CSP/Criminal/PDFs/EWSC-2016-CRIM-Page-1-Trend.ashx

Cribb, R., and J. Rankin, "420,000 in Police Database Never Convicted: Analysis," *The Star*, May 24, 2014. As of October 11, 2018: https://www.thestar.com/news/canada/2014/05/24/420000_in_police_database_never_convicted_analysis.html

Criminaliteit in Beeld, "Opsporing: bronnen en methoden," 2018. As of October 29, 2018: https://www.criminaliteitinbeeld.nl/bronnen-en-methoden/opsporing

Criminal Justice Inspectorates, homepage, n.d. As of August 14, 2019: https://www.justiceinspectorates.gov.uk

Crown Prosecution Service, "About CPS," n.d. As of June 10, 2019: https://www.cps.gov.uk/about-cps

CSC—*See* Correctional Service Canada.

Daly, K., and R. Sarre, "Criminal Justice System: Aims and Processes," in D. Palmer, W. de Lint, and D. Dalton, eds., *Crime and Justice: A Guide to Criminology*, 5th ed., Sydney: Lawbook Co., 2017.

Data.gov.uk, "Criminal Court Statistics," 2018. As of February 13, 2019: https://data.gov.uk/dataset/fdf8acba-c5ae-47c2-a1fd-0290b17b3f27/criminal-court-statistics

DBS—*See* Disclosure and Barring Service.

Decae, R. J., and C. P. M. Netten, "Vervolging," in S. N. Kalidien, ed., *Criminaliteit en rechtshandhaving 2017: Ontwikkelingen en samenhangen. WODC, CBS, and Raad vor de rechtspraak*, The Hague: WODC, 2018, pp. 57–62. As of October 27, 2018: https://www.cbs.nl/nl-nl/publicatie/2018/42/criminaliteit-en-rechtshandhaving-2017

Department of Justice, "Making the Links in Family Violence Cases: Collaboration Among the Family, Child Protection and Criminal Justice Systems; Chapter3—Impact of Pre-existing Orders and Proceedings," 2016. As of October 11, 2018: http://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/mlfvc-elcvf/p5.html

———, "The Judicial Structure," 2017a. As of October 11, 2018: http://www.justice.gc.ca/eng/csj-sjc/just/07.html

———, "The Youth Criminal Justice Act Summary and Background," 2017b. As of October 11, 2018: http://www.justice.gc.ca/eng/cj-jp/yj-jj/tools-outils/back-hist.html

Deutscher Bundestag, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Sevim Dağdelen, Kersten Naumann und der Fraktion DIE LINKE.—Drucksache 16/13319—Beim Bundeskriminalamt geführte "Gewalttäter"- und andere Dateien, June 23, 2009. As of August 13, 2019: http://dip21.bundestag.de/dip21/btd/16/135/1613563.pdf

Dienst Justitiële Inrichtingen, "3 Reclasseringsorganisaties (3RO)," n.d.a. As of October 29, 2018: https://www.forensischezorg.nl/introductie/keten-forensische-zorg/3-reclasseringsorganisaties-3ro

———, "Custodial Institutions Agency," n.d.b. As of October 29, 2018: https://www.dji.nl/english/index.aspx.

———, *This Is the Custodial Institutions Agency (DJI). In Facts and Figures, Based on 2018*, March 2019. As of August 21, 2019: https://www.dji.nl/binaries/Dit%20is%20DJI%20maart%202019%20Engels_tcm41-121757.pdf

Disclosure and Barring Service, "DBS Filtering Guide," n.d. As of June 10, 2019: https://www.gov.uk/government/publications/dbs-filtering-guidance/dbs-filtering-guide

DJI—*See* Dienst Justitiële Inrichtingen.

Drake, E. K., and D. Fumia, "Evolution of Correctional Education Evaluations and Directions for Future Research," *Criminology & Public Policy*, Vol. 16, No. 2, 2017, pp. 549–561.

Dubber, M., "The Legality Principle in American and German Criminal Law: An Essay in Comparative Legal History," in G. Martyn, A. Musson, and H. Pihlajamäki, eds., *From the Judge's Arbitrium to the Legality Principle: Legislation as a Source of Law in Criminal Trials*, Berlin: Duncker & Humblot, 2013, pp. 365–385.

Durnian, L., "The Rise of the Guilty Plea," The Prosecution Project, Research Brief 14, June 27, 2015. As of June 10, 2019: https://prosecutionproject.griffith.edu.au/the-rise-of-the-guilty-plea/

EC—*See* European Commission.

ECRIS Support Programme, *European Criminal Records Information System: Non-Binding Manual for Practitioners*, Brussels: Council of the European Union, October 8, 2013. As of August 13, 2019: https://www.ird.lt/uploads/documents/files/tarptautinis-bendradarbiavimas/keitimasis-teistumo-duomenimis-su-uzsienio-salimis/ecris/Revised_Manual_for_Practitioners_FINAL_v1_2.pdf

European Commission, "European Criminal Records Information System," n.d. As of August 13, 2019: http://ec.europa.eu/justice/criminal/european-e-justice/ecris/index_en.htm

———, "Commission Staff Working Document Accompanying the Document *Report from the Commission to the European Parliament and the Council Concerning the Exchange Through the European Criminal Records Information System (ECRIS) of Information Extracted from Criminal Records Between the Member States*," Strasbourg: European Commission, January 19, 2016.

———, *Report from the Commission to the European Parliament and the Council Concerning the Exchange Through the European Criminal Records Information System (ECRIS) of Information Extracted from Criminal Records Between the Member States*, Brussels: European Commission, June 29, 2017.

European E-Justice Portal, "Netherlands," n.d. As of February 27, 2018: https://e-justice.europa.eu/content_criminal_records-95-nl-en.do?member=1

Farrington, D. P. "Self-Reported and Official Offending from Adolescence to Adulthood," in M. W. Klein, ed., *Cross-National Research in Self-Reported Crime and Delinquency*, NATO ASI Series (Series D: Behavioural and Sciences), Vol. 50, Dordrecht: Springer, 1989, pp. 399–423.

Farrington, D. P., A. R. Piquero, and W. G. Jennings, *Offending from Childhood to Late Middle Age: Recent Results from the Cambridge Study in Delinquent Development*, New York: Springer, 2013.

Federal Bureau of Investigation, "FBI Releases 2017 Crime Statistics," press release, Washington, D.C., September 24, 2018. As of February 14, 2019: https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-2017-crime-statistics

Field, M. A., "The Differing Federalisms of Canada and the United States," *Law and Contemporary Problems*, Vol. 55, No. 1, 1992, pp. 107–120.

Fitzgerald O'Reilly, M., "The Role of Criminal Record in Bail," in *Uses and Consequences of a Criminal Conviction*, London: Palgrave Macmillan, 2018, pp. 83–104.

Flex-I.D., "Software voor opsporing & justitie," 2018. As of October 29, 2018: http://www.flex-id.nl/Software.html

Friendship, C., D. Thornton, M. Erikson, and A. Beech, "Reconviction: A Critique and Comparison of Two Main Data Sources in England and Wales," *Legal and Criminological Psychology*, Vol. 6, No. 1, 2001, pp. 121–129.

Gillespie, R. W., "Fines as an Alternative to Incarceration: The German Experience," *Federal Probation*, Vol. 44, 1980, pp. 20–26.

Goggins, B. R., and D. A. DeBacco, *Survey of State Criminal History Information Systems, 2016: A Criminal Justice Information Policy Report*, SEARCH: The National Consortium for Justice Information and Statistics, Sacramento, Calif., February 2018. As of January 28, 2019: https://www.ncjrs.gov/pdffiles1/bjs/grants/251516.pdf

Götting, B., "Das Bundeszentralregister als Instrument und Gegenstand der Forschung," in E. Hilgendorf and R. Rengier, eds., *Festschrift für Wolfgang Heinz*, Baden-Baden, Germany: Nomos Verlagsgesellschaft, 2012, pp. 84–93.

Government of Canada, "The Constitutional Distribution of Legislative Powers," n.d. As of June 10, 2019: https://www.canada.ca/en/intergovernmental-affairs/services/federation/distribution-legislative-powers.html

———, Youth Criminal Justice Act (S.C. 2002, c. 1), October 18, 2018. As of August 14, 2019: http://www.laws-lois.justice.gc.ca/eng/acts/Y-1.5/page-24.html#docCont

———, Criminal Code (R.S.C., 1985, c. C-46): Part XXVII, June 17, 2019. As of August 13, 2019: http://laws-lois.justice.gc.ca/eng/acts/C-46/page-203.html#h-287

Government of the Netherlands, "Hoe hoog zijn de boetes in Nederland?" n.d.a. As of October 27, 2018: https://www.rijksoverheid.nl/onderwerpen/straffen-en-maatregelen/vraag-en-antwoord/hoe-hoog-zijn-de-boetes-in-nederland

———, "Hoe kom ik aan een burgerservicenummer (BSN)?" n.d.b. As of October 29, 2018: https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/vraag-en-antwoord/hoe-kom-ik-aan-een-burgerservicenummer-bsn

———, "Diensten en instellingen," n.d.c. As of October 29, 2018: https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/organisatie/diensten-en-instellingen.

———, "Personal Records Database (BRP)," n.d.d. As of October 29, 2018: https://www.government.nl/topics/personal-data/personal-records-database-brp

———, "The Citizen Service Number (BSN)," n.d.e. As of October 29, 2018: https://www.government.nl/topics/personal-data/citizen-service-number-bsn

———, "The Dutch Court System," n.d.f. As of October 29, 2018: https://www.government.nl/topics/administration-of-justice-and-dispute-settlement/the-dutch-court-system

———, "Registration of Non-residents: Frequently Asked Questions," 2013. As of October 29, 2018: https://www.government.nl/documents/publications/2013/12/11/registration-of-non-residents-frequently-asked-questions

Gov.uk, "List of Offences That Will Never Be Filtered from a DBS Certificate," November 16, 2018. As of July 3, 2019: https://www.gov.uk/government/publications/dbs-list-of-offences-that-will-never-be-filtered-from-a-criminal-record-check

———, "Risk Assessment of Offenders," May 15, 2019. As of August 26, 2019: https://www.gov.uk/guidance/risk-assessment-of-offenders

Graaff-Kamphof, I. de, *The Netherland's Experience with Decentralisation*, The Hague: Ministry of Interior Affairs and Kingdom Relations, n.d. As of October 29, 2018: https://www.oecd.org/regional/regional-policy/Netherlands-experience.pdf

Heinz, W., *Das Strafrechtliche Sanktionensystem und die Sanktionierungspraxis in Deutschland 1882–2012*, January 2014. As of August 13, 2019: http://www.uni-konstanz.de/rtf/kis/Sanktionierungspraxis-in-Deutschland-Stand-2012.pdf

Helsloot, I., A. Schmidt, B. Tholen, D. de Vries, C. Grütters, and M. de Vries, *Evaluatie Wet justitiële en strafvorderlijke gegevens. In opdracht van het ministerie van Veiligheid en Justitie, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)*, The Hague, 2013. As of August 21, 2019: https://zoek.officielebekendmakingen.nl/blg-397359.pdf

Herzog-Evans, M., "Judicial Rehabilitation in Six Countries: Australia, England and Wales, France, Germany, the Netherlands and Spain," *European Journal of Probation*, Vol. 3, No. 1, 2011, pp. 1–3.

Hilton, N. Z., and A. W. Eke, Non-specialization of Criminal Careers Among Intimate Partner Violence Offenders," *Criminal Justice and Behavior*, Vol. 43, No. 10, 2016, pp. 1347–1363.

Historiek, "Trias Politica in Nederland," 2008. As of October 29, 2018: http://historiek.net/trias-politica-in-nederland/1145/

HM Government, "Prison Population Figures: 2019," 2019. As of June 10, 2019: https://www.gov.uk/government/statistics/prison-population-figures-2019

HMIC—*See* HM Inspectorate of Constabulary.

HM Inspectorate of Constabulary, "Police National Computer Audits," n.d. As of July 3, 2019: http://webarchive.nationalarchives.gov.uk/20111013165059/http://www.hmic.gov.uk/inspections/police-national-computer-audits/

———, *Crime Recording: A Matter of Fact; an Interim Report of the Inspection of Crime Data Integrity in Police Forces in England and Wales*, London: HMIC, 2014. As of July 3, 2019: https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/2014/05/crime-data-integrity-interim-report.pdf

HM Prison Service, "About Us," n.d. As of June 10, 2019: https://www.gov.uk/government/organisations/hm-prison-service/about

Home Office, *Nominal Criminal Records on the Police National Computer*, FOI release, London, January 21, 2015. As of June 10, 2019: https://www.gov.uk/government/publications/nominal-criminal-records-on-the-police-national-computer/nominal-criminal-records-on-the-police-national-computer

Huey, L., "Why Data?" Canadian Society of Evidence Based Policing (blog), March 4, 2017. As of October 11, 2018: http://www.can-sebp.net/single-post/2017/03/02/Why-data

Immigration, Refugees and Citizenship Canada, "Information for Canadian Law Enforcement," 2016. As of October 11, 2018: https://www.canada.ca/en/immigration-refugees-citizenship/services/canadian-passports/security/police-information.html

Information Commissioner's Officer, "Guide to Data Protection," n.d. As of June 10, 2019: https://ico.org.uk/for-organisations/guide-to-data-protection-404/

Jackson, A. M., and G. L. Davies, "Making the Case for ECRIS: Post-'Brexit' Sharing of Criminal Records Information Between the European Union and United Kingdom," *The International Journal of Evidence & Proof*, Vol. 21, No. 4, 2017, pp. 330–350.

Jacobs, J., and E. Larrauri, "European Criminal Records & Ex-Offender Employment," New York, New York University Public Law and Legal Theory Working Papers 10-2015, October 2015. As of January 28, 2019: https://lsr.nellco.org/cgi/viewcontent.cgi?referer=http://scholar.google.com/&httpsredir=1&article=1532&context=nyu_plltwp

Jacobs, J. B., "Mass Incarceration and the Proliferation of Criminal Records," *University of St. Thomas Law Journal*, Vol. 3, No. 3, 2006, pp. 387–420.

———, *The Eternal Criminal Record*, Cambridge, Mass.: Harvard University Press, 2015.

Janus, E. S., S. Alexander, and L. Graf, "M. v. Germany: The European Court of Human Rights Takes a Critical Look at Preventive Detention," *Arizona Journal of International and Comparative Law*, Vol. 29, No. 3, 2012, pp. 605–622.

Jehle, J.-M., "Germany," in M. Aebi and V. Jaquier, eds., *Crime and Punishment Around the World*, Santa Barbara, Calif.: ABC-CLIO-Verlag, 2010, pp. 123–132.

———, "Approach, Structure and Outcome of the German Reconviction Study," in J.-M. Jehle and H.-J. Albrecht, eds., *National Reconviction Statistics and Studies in Europe*, Vol. 25, Göttingen Studies in Criminal Law and Justice, Göttingen, Germany: Universitätsverlag Göttingen, 2014, pp. 25–43.

———, *Criminal Justice in Germany*, 6th ed., Berlin: Federal Ministry of Justice and Consumer Protection, 2015.

Jehle, J.-M., H.-J. Albrecht, S. Hohmann-Fricke, and C. Tetal (2016), *Legalbewährung nach strafrechtlichen Sanktionen: Eine bundesweite Rückfalluntersuchung 2010 bis 2013 und 2004 bis 2013*, Berlin: Ministry of Justice and Consumer Protection, 2016. As of November 4, 2018: https://www.uni-goettingen.de/de/legalbew%c3%a4hrung+nach+strafrechtlichen+sanktionen+2010+bis+2013+und+2004+bis+2013/553646.html

Judicial Office International Team, *The Judicial System of England and Wales: A Visitor's Guide*, London: Judicial Office, 2016. As of July 3, 2019: https://www.judiciary.uk/wp-content/uploads/2016/05/international-visitors-guide-10a.pdf

JustID, "Dienstverlening," n.d.a. As of October 29, 2018: https://www.justid.nl/dienstverlening/

———, "Informatieverstrekking," n.d.b. As of October 29, 2018: https://www.justid.nl/organisatie/JDS/Informatieverstrekking.aspx

———, "Inzage en correctie," n.d.c. As of October 29, 2018: https://www.justid.nl/organisatie/JDS/Inzageencorrectie.aspx.

———, "Persoonsdossier Systeem (PDS)," n.d.d. As of October 29, 2018: https://www.justid.nl/organisatie/JDS/PersoonsdossierSysteemPDS.aspx

———, "Registratie en bewaartermijnen," n.d.e. As of October 29, 2018: https://www.justid.nl/organisatie/JDS/registratie.aspx

———, *Justitieel Documentatie Systeem (JDS)*, Almelo, Netherlands, March 13, 2009. As of October 29, 2018: https://www.justid.nl/binaries/facsheet-jds_tcm17-21493.pdf.

———, *Factsheet ID-staat Strafrechtsketendatabank (SKDB) met uitleg*, Almelo, Netherlands, January 2011. As of August 14, 2019: https://www.justid.nl/binaries/factsheet-id-staat-skdb-2012_tcm17-21327.pdf

———, *Justitiële Informatiedienst Informeert*, Almelo, Netherlands, March 2017a. As of October 27, 2018: https://www.justid.nl/binaries/Nieuwsbrief%20Justiti%C3%ABle%20Informatiedienst%20maart%202017_tcm17-253249.pdf

———, "Presentatie Justitiële Documentatie," 2017b, internal document.

Justis, "De VOG beoordeling in het kort," n.d.a. As of October 27, 2018: https://www.justis.nl/producten/vog/vog-beoordeling-in-het-kort/de-vog-beoordeling-in-het-kort.aspx

———, "FAQ: After You Apply," n.d.b. As of October 27, 2018: https://www.justis.nl/producten/vog/certificate-of-conduct/after-you-apply/faq-after-you-apply.aspx

———, "Terugkijktermijnen," n.d.c. As of October 27, 2018: https://www.justis.nl/producten/vog/vog-aanvragen/naar-welke-gegevens-wordt-gekeken/terugkijktermijnen.aspx

———, “Veelgestelde vragen over de elektronische VOG-aanvraag voor werknemers,” n.d.d. As of October 27, 2018: https://www.justis.nl/producten/vog/faq/faq-over-elektronische-vog-aanvraag/index.aspx

———, “VOG voor natuurlijke personen (VOG NP),” n.d.e. As of October 27, 2018: https://www.justis.nl/producten/vog/waarvoor-heeft-u-een-vog-nodig/vog-np.aspx

———, “Waarvoor heeft u een VOG nodig?” n.d.f. As of October 27, 2018: https://www.justis.nl/producten/vog/waarvoor-heeft-u-een-vog-nodig/index.aspx

———, “Wat is een VOG?” n.d.g. As of October 27, 2018: https://www.justis.nl/producten/vog/index.aspx

———, “Application Form: Certificate of Conduct for Natural Persons (VOG NP),” January 2017. As of August 21, 2019: https://www.justis.nl/binaries/Aanvraagformulier%20VOG%20NP%20(Engels)%20Januari%202017_tcm34-84796.pdf

———, “Verklaring Omtrent het Gedrag: Screeningsprofielen VOG NP,” January 2018. As of August 21, 2019: https://www.justis.nl/binaries/WEB_110055_Screeningsprofielen_VOG%20NP_DEF_tcm34-371057.pdf

Kaeble, D., and M. Cowhig, *Correctional Populations in the United States, 2016*, Washington, D.C., Bureau of Justice Statistics, NCJ 251211, 2018. As of February 13, 2019: https://www.bjs.gov/content/pub/pdf/cpus16.pdf

Kilgour, L., “Tracing the Lifecycle of Canadian Criminal Records: A Critical Examination in Relation to Public Policy and User Access and Comprehension,” *Records Management Journal*, Vol. 23, No. 2, 2013, pp. 136–148.

Kim, J., P. Chauhan, O. Lu, M. Patten, and S. S. Smith, “Unpacking Pretrial Detention: An Examination of Patterns and Predictors of Readmissions,” *Criminal Justice Policy Review*, Vol. 29, No. 6–7, 2018, pp. 663–687.

King, A., *Does the United Kingdom Still Have a Constitution?* London: Sweet & Maxwell, 2001. As of June 10, 2019: https://socialsciences.exeter.ac.uk/media/universityofexeter/schoolofhumanitiesandsocialsciences/law/pdfs/Does_the_United_Kingdom_still_have_a_constitution.pdf

Krehl, C., “Reforms of the German Criminal Code—Stock-Taking and Perspectives—also from a Constitutional Point of View,” *German Law Journal*, Vol. 4, No. 5, 2003, p. 421.

Kruize, P., and P. Gruter, *Eens Een Dief, Altijd Een Dief? Een Verkenning Rond het Meten van de Effectiviteit van de Verklaring Omtrent het Gedrag*, The Hague, Netherlands: Ministerie van Veiligheid en Justitie, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC),

2016. As of November 6, 2018:
https://www.njb.nl/Uploads/2017/2/eens-een-dief-altijd-een-dief.pdf

Kurtovic, E., and M. Rovira, "Contrast Between Spain and the Netherlands in the Hidden Obstacles to Re-entry into the Labour Market due to a Criminal Record," *European Journal of Criminology*, Vol. 14, No. 5, 2017, pp. 505–521.

Lapp, K., "American Criminal Record Exceptionalism," *Ohio State Journal of Criminal Law*, Vol. 14, 2016, p. 303.

Larrauri, E., "Criminal Record Disclosure and the Right to Privacy," *Criminal Law Review*, Vol. 10, 2014, pp. 723–737.

Law Enforcement Information Network, "Canadian Police Information Centre (CPIC) Access," correspondence, Lansing, Mich., December 4, 2015. As of October 11, 2018:
https://www.michigan.gov/documents/msp/LEIN_Training_Bulletin_-_CPIC_Access_507637_7.pdf

Legislation.gov.uk, "Police and Criminal Evidence Act 1984," n.d. As of July 3, 2019.
https://www.legislation.gov.uk/ukpga/1984/60/section/27

Legislative Assembly of the Northwest Territories, "Differences from Provincial Governments," n.d. As of June 10, 2019:
https://www.assembly.gov.nt.ca/visitors/what-consensus/differences-provincial-governments

Leij, J. B. J. van der, "Het Nederlandse strafrechtssyteem," in *Criminaliteit en Rechtshandhaving 2013, Ontwikkelingen en samenhangen*, Justitie in statistiek 4, The Hague: Boom Lemma, 2014, pp. 21–57.

Love, M., "Starting Over with a Clean Slate," *Fordham Urban Law Journal*, Vol. 30, 2002, pp. 1705–1741.

Malakieh, J., "Adult and Youth Correctional Statistics in Canada, 2016/2017," Statistics Canada, June 19, 2018. As of October 11, 2018:
https://www150.statcan.gc.ca/n1/pub/85-002-x/2018001/article/54972-eng.htm

Marshall, W. L., "A Brief History of Psychological Theory, Research, and Treatment with Adult Male Sex Offenders," *Current Psychiatry Reports*, Vol. 20, No. 8, 2018, p. 57.

Maruna, S., "Judicial Rehabilitation and the 'Clean Bill of Health' in Criminal Justice," *European Journal of Probation*, Vol. 3, 2011, pp. 97–117.

Mathesius, J., and P. Lussier, "The Successful Onset of Sex Offending: Determining the Correlates of Actual and Official Onset of Sex Offending," *Journal of Criminal Justice*, Vol. 42, 2014, pp. 134–144.

Maxwell, A., "Adult Criminal Court Statistics in Canada, 2014/2015," Statistics Canada, February 21, 2017. As of October 11, 2018: https://www150.statcan.gc.ca/n1/pub/85-002-x/2017001/article/14699-eng.htm

McCormick, A.V., T. Haarhoff, I. M. Cohen, D. Plecas, and K. Burk, *Challenges Associated with Interpreting and Using Police Clearance Rates*, Centre for Public Safety and Criminal Justice Research, University of the Fraser Valley, 2007. As of October 11, 2018: https://www.ufv.ca/media/assets/ccjr/reports-and-publications/Clearance_Rate_Report_2012.pdf

Ministry of Justice, *Justice Data Lab Pilot Summary*, London, June 11, 2015. As of August 14, 2019: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434165/justice-data-lab-pilot-summary.pdf

———, *Guide to Proven Reoffending Statistics*, London, January 2018. As of August 14, 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/676411/guide-to-proven-reoffending-statistics-jan18.pdf

———, *Criminal Justice Statistics Quarterly, England and Wales, Year Ending December 2018 (Annual)*, May 16, 2019. As of June 10, 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/802032/criminal-justice-statistics-quarterly-december-2018.pdf

Model, O., and C. Creifelds, *Staatsbürger-Taschenbuch Alles Wissenswerte über Europa, Staat, Verwaltung, Recht und Wirtschaft mit zahlreichen Schaubildern*, 34th ed., Munich: C. H. Beck, 2017.

MOJ—*See* Ministry of Justice.

Monahan, J., and J. L. Skeem, "Risk Assessment in Criminal Sentencing," *Annual Review of Clinical Psychology*, Vol. 12, 2016, pp. 489–513.

Morgenstern, C., and E. M. Arndt, "Judicial Rehabilitation in Germany—the Use of Criminal Records and the Removal of Recorded Convictions," *European Journal of Probation*, Vol. 3, No. 1, 2011, pp. 20–35.

Myrent, M., *Using State Criminal History Records for Research and Evaluation*, Justice Research and Statistics Association, Washington, D.C., June 2019. As of July 15, 2019: http://www.jrsa.org/pubs/factsheets/jrsa-factsheet-chri.pdf

National Police Chiefs' Council, *Deletion of Records from National Police Systems (PNC/NDNAD/IDENT1)*, October 18, 2018. As of June 10, 2019: https://www.acro.police.uk/uploadedFiles/Deletion%20of%20Records%20from%20National%20Police%20Systems%20(Guidance)%20v2.0.pdf

Nederlands Forensisch Instituut, "Nederlandse DNA-databank," n.d. As of July 15, 2019: https://dnadatabank.forensischinstituut.nl/dna-databanken

Neighly, M., and M. Emsellem, *Wanted: Accurate FBI Background Checks for Employment*. National Employment Law Project, New York, July 2013. As of January 28, 2019: https://nelp.org/wp-content/uploads/2015/03/Report-Wanted-Accurate-FBI-Background-Checks-Employment.pdf

Netherlands Institute for Multiparty Democracy and Instituut voor Publiek en Politiek, *The Dutch Political System in a Nutshell*, The Hague: Instituut voor Publiek en Politiek, 2008.

NPCC—*See* National Police Chiefs' Council.

OAG—*See* Office of the Auditor General of Canada.

OAIC—*See* Office of the Australian Information Coordinator.

Office for National Statistics, "Population Estimates," 2018. As of June 10, 2019: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates

———, "Crime in England and Wales: Year Ending December 2018," 2019. As of June 10, 2019: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2018

Office of the Auditor General of Canada, "2009 March Status Report of the Auditor General of Canada," 2009. As of October 11, 2018: http://www.oag-bvg.gc.ca/internet/English/parl_oag_200903_01_e_32288.html

———, "2011 June Status Report of the Auditor General of Canada," 2011. As of October 11, 2018: http://www.oag-bvg.gc.ca/internet/English/parl_oag_201106_e_35354.html

Office of the Australian Information Coordinator, "Australian Privacy Principles," n.d. As of July 3, 2019: https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles

Office of the Privacy Commissioner of Canada, *Audit of Selected RCMP Operational Databases*, Ottawa, Ontario, 2011. As of October 11, 2018: https://www.priv.gc.ca/media/1148/ar-vr_rcmp_2011_e.pdf

———, "Disclosure of Information About Complainant's Attempted Suicide to US Customs and Border Protection Not Authorized Under the Privacy Act," 2017. As of November 4, 2018: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170419_rcmp/

OM—*See* Openbaar Ministerie.

ONS—*See* Office for National Statistics.

OPC—*See* Office of the Privacy Commissioner of Canada.

Openbaar Ministerie, "Organisatie," n.d.a. As of October 29, 2018: https://www.om.nl/organisatie/

———, "Organogram," n.d.b. As of October 29, 2018: https://www.om.nl/organisatie/organogram/

Overheid.nl, "Wet justitiële en strafvorderlijke gegevens," 2016. As of October 29, 2018: http://wetten.overheid.nl/BWBR0014194/2016-01-01

Parliament of Canada, Royal Assent to the 2006 Director of Public Prosecution Act, Bill C-2, December 12, 2006. As of October 11, 2018: http://www.parl.ca/DocumentViewer/en/39-1/bill/C-2/royal-assent/page-290#28

Parole Board of Canada, "Record Suspension Program 2015–2016 Report to Parliament," 2016a. As of October 11, 2018: https://www.canada.ca/en/parole-board/corporate/transparency/reporting-to-canadians/record-suspension-report-to-parliament-2015-2016.html

———, "Statistics: Parole, Pardons and Clemency," 2016b. As of October 11, 2018: https://www.canada.ca/en/parole-board/corporate/publications-and-forms/fact-sheets/statistics-parole-pardons-and-clemency.html

———, *Record Suspension Guide*, 2018. As of August 21, 2019: https://www.canada.ca/content/dam/pbc-clcc/documents/form-formulaire/rs-sc/PBC_Record_Suspension_Application_Guide_072019.pdf

———, *Decision-Making Policy Manual for Board Members*, June 21, 2019. As of August 21, 2019: https://www.canada.ca/en/parole-board/corporate/publications-and-forms/decision-making-policy-manual-for-board-members.html

PBC—*See* Parole Board of Canada

Pfeiffer, J., "Die unbeschränkte Auskunft aus dem Bundeszentralregister und das Führungszeugnis," *Neue Zeitschrift für Strafrecht*, Vol. 20, 2000, pp. 402–405.

Pijoan, E. L., "Legal Protections Against Criminal Background Checks in Europe," *Punishment & Society*, Vol. 16, No. 1, 2014, pp. 50–73.

Politie, "Geschiedenis," n.d.a. As of October 29, 2018: https://www.politie.nl/over-de-politie/organisatie---geschiedenis.html.

———, "Organisatie," n.d.b. As of October 29, 2018: https://www.kombijdepolitie.nl/over-ons/Paginas/organisatie.aspx

———, "Organisatie: één politie, elf eenheden," n.d.c. As of October 29, 2018: https://www.politie.nl/over-de-politie/een-politie-elf-eenheden.html

———, *Bijlage Inrichtingsplan Nationale Politie*, December 2012. As of October 29, 2018: https://zoek.officielebekendmakingen.nl/blg-198148.pdf

———, "Meer geld nodig voor operationele ICT-systemen politie," Politie, April 11, 2017. As of August 14, 2019: https://www.politie.nl/nieuws/2017/november/4/00-meer-geld-nodig-voor-operationele-ict-systemen-politie.html

PPSC—*See* Public Prosecution Service of Canada.

Public Prosecution Service of Canada, "About the Public Prosecution Service of Canada," 2018. As of October 11, 2018: http://www.ppsc-sppc.gc.ca/eng/bas/index.html#mandate

RCMP—*See* Royal Canadian Mounted Police.

Rechtspraak, "The Judicial System," 2017. As of October 29, 2018: https://www.rechtspraak.nl/English

Roxin, C., G. Arzt, and K. Tiedemann, *Einführung in das Strafrecht und Strafprozessrecht*, 6th ed., Heidelberg, Germany: C. F. Muller, 2014.

Royal Canadian Mounted Police, *RCMP Canadian Firearms Program: Program Evaluation: Final Approved Report*, February 2010. As of October 11, 2018: http://www.rcmp-grc.gc.ca/pubs/fire-feu-eval/eval-eng.pdf

———, "Status Report on Transformational and Major Crown Projects," 2013. As of October 11, 2018: http://www.rcmp-grc.gc.ca/en/status-report-transformational-and-major-crown-projects

———, "Compelling Reasons to Deny a Request for Destroying Non-conviction Information," 2014a. As of October 11, 2018: http://www.rcmp-grc.gc.ca/en/compelling-reasons-deny-request-destroying-non-conviction-information

———, "Dissemination of Criminal Record Information Policy," 2014b. As of October 11, 2018: http://www.rcmp-grc.gc.ca/en/dissemination-criminal-record-information-policy

———, "Follow-Up to the Office of the Privacy Commissioner's Audit of the Security of Personal Information," 2016a. As of October 11, 2018: http://www.rcmp-grc.gc.ca/en/follow-the-office-the-privacy-commissioners-audit-the-security-personal-information

———, *Report on Plans and Priorities 2016–2017*, 2016b. As of October 11, 2018: http://publications.gc.ca/collections/collection_2016/grc-rcmp/PS61-20-2016-eng.pdf

———, “Response to an Access to Information Act Request A-2016-05604/F141,” 2016c. As of August 5, 2017: http://dennisryoung.ca/2017/01/08/rcmp-report-cpic-backlog-of-550639-fingerprint-files/

———, “Royal Canadian Mounted Police 2015–16 Departmental Performance Report,” 2016d. As of October 11, 2018: http://www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-2015-16-departmental-performance-report

———, “About the RCMP,” 2018a. As of October 11, 2018: http://www.rcmp-grc.gc.ca/about-ausujet/index-eng.htm

———, “Managing Criminal Records,” 2018b. As of October 11, 2018: http://www.rcmp-grc.gc.ca/en/managing-criminal-records

Satzger, H., W. Schluckebier, and G. Widmaier, *Strafprozessordnung mit GVG und EMRK: Kommentar*, 2nd ed., Cologne, Germany: Carl Heymanns Verlag, 2016.

Senate of Canada, “Meeting of the Standing Senate Committee on Legal and Constitutional Affairs, 26 October 2016,” 2016. As of October 11, 2018: https://sencanada.ca/en/Content/Sen/committee/421/lcjc/52843-e

Sentencing Advisory Council, “Guilty Pleas and Sentencing,” 2018. As of June 10, 2019: https://www.sentencingcouncil.vic.gov.au/about-sentencing/sentencing-process/guilty-pleas-and-sentencing

Sentencing Council, “Discharges,” n.d.a. As of June 10, 2019: https://www.sentencingcouncil.org.uk/about-sentencing/types-of-sentence/discharges/

———, “Introduction to Compensation,” n.d.b. As of June 10, 2019: https://www.sentencingcouncil.org.uk/explanatory-material/magistrates-court/item/fines-and-financial-orders/compensation/1-introduction-to-compensation/

———, “Suspended Sentences,” n.d.c. As of June 10, 2019: https://www.sentencingcouncil.org.uk/about-sentencing/types-of-sentence/suspended-sentences/

Siegismund, E., “The Public Prosecution Office in Germany: Legal Status, Functions and Organization,” in *Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (2003) Annual Report for 2001 and Resource Material Series No. 60*, 2003. As of August 21, 2019: https://www.unafei.or.jp/publications/pdf/RS_No60/No60_10VE_Siegismund2.pdf

Smit, P. R., and R. J. Kessels, “Misdrijven en opsporing,” in S. N. Kalidien, ed., *Criminaliteit en rechtshandhaving 2017: Ontwikkelingen en samenhangen. WODC, CBS, and Raad vor de*

rechtspraak, The Hague: WODC, 2018, pp. 51–56. As of October 27, 2018: https://www.cbs.nl/nl-nl/publicatie/2018/42/criminaliteit-en-rechtshandhaving-2017

Spohn, C., "Evolution of Sentencing Research," *Criminology & Public Policy*, Vol. 14, No. 2, 2015, pp. 225–232.

Staatscourant, *Beleidsregels VOG-NP-RP 2018. Nr. 68620*, December 1, 2017. As of October 27, 2018: https://www.justis.nl/binaries/stcrt-2017-68620%20Beleidsregels%202018_tcm34-296654.pdf

Statistics Canada, "Population Estimates on July 1st, by Age and Sex," 2018. As of October 11, 2018: https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1710000501

Statistisches Bundesamt, *Bevölkerung und Erwerbstätigkeit: Bevölkerung mit Migrationshintergrund—Ergebnisse des Mikrozensus 2017*, August 2018a. As of June 13, 2019: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Migration-Integration/Publikationen/Downloads-Migration/migrationshintergrund-2010220177004.pdf?__blob=publicationFile&v=4

———, "Justiz und Rechtspflege: Strafverfolgung. Fachserie 10 Reihe 3," 2018b. As of June 10, 2019: https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/_inhalt.html?nn=72374

———, "Schätzung für 2018: Bevölkerungszahl auf 83,0 Millionen gestiegen," press release, Wiesbaden, Germany, January 25, 2019a. As of June 13, 2019: https://www.destatis.de/DE/Presse/Pressemitteilungen/2019/01/PD19_029_12411.html

———, "Bestand der Gefangenen und Verwahrten in den deutschen Justizvollzugsanstalten nach ihrer Unterbringung auf Haftplätzen des geschlossenen und offenen Vollzugs jeweils zu den Stichtagen 31. März, 31. August und 30. November eines Jahres; Stichtag 30. November 2018," Statistisches Bundesamt (Destatis), March 25, 2019b. As of August 21, 2019: https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Strafverfolgung-Strafvollzug/bestand-gefangene-verwahrte-pdf-5243201.pdf?__blob=publicationFile

Tak, J. P., *The Dutch Criminal Justice System. Organization and Operation. Onderzoek en Beleid, 205*, 2nd rev. ed., The Hague: WODC, 2003.

Tolzmann, G., *Bundeszentralregistergesetz: Zentralregister, Erziehungsregister, Gewerbezentral*, 5th ed., Stuttgart, Germany: Kohlhammer Verlag, 2015.

Topfer, E., *A Network Being Networked: The Databases of Germany's Federal Criminal Police Office*, 2009. As of August 14, 2019: https://www.burojansen.nl/pdf/StatewatchBKADatabaseNet.pdf

United States Courts, "Caseload Statistics Data Tables," n.d. As of February 13, 2019: https://www.uscourts.gov/statistics-reports/caseload-statistics-data-tables?tn=&pn=All&t=69&m%5Bvalue%5D%5Bmonth%5D=&y%5Bvalue%5D%5Byear%5D=&=Apply

Valkhoff, J., "Nationale Politie: 10 regio's en 43 districten," Gemeente.nu, June 26, 2012. As of October 29, 2018: https://www.gemeente.nu/bestuur/gemeenten/nationale-politie-10-regios-en-43-districten/

Vink, M. E., and S. W. van den Braak, "Berechting," in S. N. Kalidien, ed., *Criminaliteit en rechtshandhaving 2017: Ontwikkelingen en samenhangen. WODC, CBS, and Raad vor de rechtspraak*, The Hague: WODC, 2018, pp. 63–70. As of October 27, 2018: https://www.cbs.nl/nl-nl/publicatie/2018/42/criminaliteit-en-rechtshandhaving-2017

Vuolo, M., S. Lageson, and C. Uggen, "Criminal Record Questions in the Era of 'Ban the Box,'" *Criminology & Public Policy*, Vol. 16, No. 1, 2017, pp. 139–165.

Waard, J. de, *Daling van (geregistreerde) criminaliteit: Trends en mogelijke verklaringen*, The Hague: Ministerie van Veiligheid en Justitie, Directie Rechtshandhaving en Criminaliteitsbestrijding, 2015.

———, "Criminology's Dirty Little Secret: Hoe de daling van de criminaliteit bijna geheel voorbijging aan de Nederlandse criminologie," in Bijleveld, C., and P. van der Laan, eds., *Liber Amicorum Gerben Bruinsma*, The Hague: Boom Criminologie, 2017, pp. 333–345.

Wartna, B. S., J. M. Blom, and N. Tollenaar, *The Dutch Recidivism Monitor*, 4th rev. ed., The Hague: Research and Documentation Centre, Ministry of Security and Justice, 2011.

Wheeler, A. P., R. E. Worden, and S. J. McLean, "Replicating Group-Based Trajectory Models of Crime at Micro-Places in Albany, NY," *Journal of Quantitative Criminology*, Vol. 32, No. 4, 2016, pp. 589–612.

Windsor Police Service, "CPIC/Charge Processing Unit," n.d. As of October 11, 2018: https://www.police.windsor.on.ca/what-we-do/operational-support/information-services/Pages/CPIC-Charge-Processing-Unit.aspx

Youth Justice Legal Centre, "Spent Conviction," January 9, 2015. As of August 14, 2019: http://www.yjlc.uk/spent-conviction

Yukon Legislative Assembly, *Information Sheet No. 7: The Differences Between Provinces and Territories*, September 17, 2012. As of June 10, 2019: http://www.legassembly.gov.yk.ca/pdf/7_diff_between_prov_territories.pdf