



IACP TECHNOLOGY POLICY FRAMEWORK¹

January 2014

Introduction

New and emerging technologies increasingly play a crucial role in the daily work of police, equipping officers with enforcement and investigative tools that have the potential of making them safer, better informed, and more effective and efficient. Developing and enforcing comprehensive agency policies regarding deployment and use is a critical step in realizing the value that technologies promise, and is essential in assuring the public that their privacy and civil liberties are recognized and protected.

Technological advances have made it possible to monitor and record nearly every interaction between police and the public through the use of in-car and body-worn video, access to an expanding network of public and private video surveillance systems, and the increasing use of smartphones with digital recording capabilities by citizens and officers alike. Police can track suspects with the use of GPS tracking technologies and officers themselves can be tracked with automated vehicle location (AVL) systems. Automated license plate recognition (ALPR) systems can scan the license plates of vehicles within sight of officers in the field and quickly alert them if the vehicle has been reported stolen or is wanted. Identity can be remotely verified or established with biometric precision using mobile fingerprint scanners and facial recognition software. Crimes can be mapped as they are reported, gunshot detection technology can alert law enforcement almost instantaneously when a firearm is discharged, and surveillance cameras can be programmed to focus in on the gunshot location and stream live video to both dispatchers and responding officers. With these advancements come new opportunities to enhance public and officer safety. They also present new challenges for law enforcement executives.

The challenges include identifying which technologies can be incorporated by the agency to achieve the greatest public safety benefits, and defining metrics that will enable the agency to monitor and assess the value and performance of the technologies. Just because a technology *can* be implemented, does not mean that it *should* be. There are also challenges in integrating these technologies across different platforms, building resilient infrastructure and comprehensive security, providing technical support, and maintaining and upgrading applications and hardware. All of this can be confusing and technically demanding, underscoring the need for effective planning, strategic deployment, and performance management.

Addressing these challenges is paramount because of the broader issues that the use of this expanding array of technologies by law enforcement presents. A principal tenet of policing is the trust citizens grant police to take actions on their behalf. If that trust is violated and public approval lost, police are not able to effectively perform their duties to keep communities safe.

The Policy Mandate

Creating and enforcing agency policies that govern the deployment and use of technology, protecting the civil rights and civil liberties of individuals, as well as the privacy protections afforded to the data collected, stored, and used, is essential to ensure effective and sustainable implementation, and to maintain community trust. Policies function to reinforce training and to establish an operational baseline to guide officers and other personnel in proper procedures regarding its use. Moreover, policies help to ensure uniformity in practice across the agency and to enforce accountability. Policies should reflect the mission and values of the agency and be tightly aligned with applicable local, state, and federal laws, regulations, and judicial rulings.

Policies also function to establish transparency of operations, enabling agencies to allay public fears and misperceptions by providing a framework that ensures responsible use, accountability, and legal and constitutional compliance. The use of automated license plate recognition (ALPR) technologies, unmanned aerial systems, and body-worn video by law enforcement, for example, has generated substantial public discussion, increasing scrutiny, and legislative action in recent years.² Privacy advocates, elected officials, and members of the public have raised important questions about how and under what circumstances these technologies are deployed, for what purposes, and how the data gathered by these technologies are retained, used, and shared. Having and enforcing a strong policy framework enables law enforcement executives to demonstrate responsible planning, implementation, and management.

Agencies should adopt and enforce a technology policy framework that addresses technology objectives, deployment, privacy protections, records management, data quality, systems security, data retention and purging, access and use of stored data, information sharing, accountability, training, and sanctions for non-compliance. Agencies should implement safeguards to ensure that technologies will not be deployed in a manner that could violate civil rights (race, religion, national origin, ethnicity, etc.) or civil liberties (speech, assembly, religious exercise, etc.). The policy framework is but one of several critical components in the larger technology planning effort that agencies should undertake to ensure proper and effective use of automation.

Universal Principles

Given the privacy concerns and sensitivity of personally identifiable information and other data often captured and used by law enforcement agencies,³ and recognizing evolving perceptions of what constitutes a reasonable expectation of privacy,⁴ the

technology policy framework should be anchored in principles universally recognized as essential in a democratic society.

The following universal principles should be viewed as a guide in the development of effective policies for *technologies that can, or have the potential to monitor, capture, store, transmit and/or share data, including audio, video, visual images, or other personally identifiable information which may include the time, date, and geographic location where the data were captured.*⁵

1. *Specification of Use*—Agencies should define the purpose, objectives, and requirements for implementing specific technologies, and identify the types of data captured, stored, generated, or otherwise produced.
2. *Policies and Procedures*—Agencies should articulate in writing, educate personnel regarding, and enforce agency policies and procedures governing adoption, deployment, use, and access to the technology and the data it provides. These policies and procedures should be reviewed and updated on a regular basis, and whenever the technology or its use, or use of the data it provides significantly changes.
3. *Privacy and Data Quality*—The agency should assess the privacy risks and recognize the privacy interests of all persons, articulate privacy protections in agency policies, and regularly review and evaluate technology deployment, access, use, data sharing, and privacy policies to ensure data quality (i.e., accurate, timely, and complete information) and compliance with local, state, and federal laws, constitutional mandates, policies, and practice.
4. *Data Minimization and Limitation*—The agency should recognize that only those technologies, and only those data, that are strictly needed to accomplish the specific objectives approved by the agency will be deployed, and only for so long as it demonstrates continuing value and alignment with applicable constitutional, legislative, regulatory, judicial, and policy mandates.
5. *Performance Evaluation*—Agencies should regularly monitor and evaluate the performance and value of technologies to determine whether continued deployment and use is warranted on operational, tactical, and technical grounds.
6. *Transparency and Notice*—Agencies should employ open and public communication and decision-making regarding the adoption, deployment, use, and access to technology, the data it provides, and the policies governing its use. When and where appropriate, the decision-making process should also involve governing/oversight bodies, particularly in the procurement process. Agencies should provide notice, when applicable, regarding the deployment and use of technologies, as well as make their privacy policies available to the public. There are practical and legal exceptions to this principle for technologies that are

lawfully deployed in undercover investigations and legitimate, approved covert operations.⁶

7. *Security*—Agencies should develop and implement technical, operational, and policy tools and resources to establish and ensure appropriate security of the technology (including networks and infrastructure) and the data it provides to safeguard against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. This principle includes meeting state and federal security mandates (e.g., the FBI’s CJIS Security Policy⁷), and having procedures in place to respond if a data breach, loss, compromise, or unauthorized disclosure occurs, including whether, how, and when affected persons will be notified, and remedial and corrective actions to be taken.⁸
8. *Data Retention, Access and Use*—Agencies should have a policy that clearly articulates that data collection, retention, access, and use practices are aligned with their strategic and tactical objectives, and that data are retained in conformance with local, state, and/or federal statute/law or retention policies, and only as long as it has a demonstrable, practical value.
9. *Auditing and Accountability*—Agencies and their sworn and civilian employees, contractors, subcontractors, and volunteers should be held accountable for complying with agency, state, and federal policies surrounding the deployment and use of the technology and the data it provides. All access to data derived and/or generated from the use of relevant technologies should be subject to specific authorization and strictly and regularly audited to ensure policy compliance and data integrity. Sanctions for non-compliance should be defined and enforced.

Developing Policies and Operating Procedures

The universal principles provide structural guidance for the development of specific agency policies and operating procedures that comport with established constitutional, legal, and ethical mandates and standards. Agency policies and procedures specify the operational components of each individual technology implementation, deployment, and management, and should typically include and address the following factors:⁹

1. Purpose
 - a. A general discussion of the purpose of a specific agency policy to include the agency’s position on protecting privacy.
2. Policy
 - a. A discussion of the overarching agency policy regarding the deployment and use of a specific technology, its application to members of the agency, and reference to relevant laws, policies, and/or regulations that authorize the agency to implement a technology, or that relate to the use and deployment of a technology.
3. Definitions

- a. A description of the technology, its components, and functions.
 - b. Definitions and acronyms associated with the technology.
4. Management
- a. Strategic Alignment: Describe how the technology aligns and furthers the agency's strategic and tactical deployment objectives.
 - b. Objectives and Performance: Identify objectives for the deployment and conditions for use of a technology, and a general strategy for assessing performance and compliance with the agency's policy.
 - c. Ownership: Clearly specify that the hardware and software associated with the technology is the property of the agency, regardless whether it has been purchased, leased, or acquired as a service, and that all deployments of a technology are for official use only (FOUO). All data captured, stored, generated, or otherwise produced by a technology are the property of the agency, regardless where the data are housed or stored. All access, use, sharing, and dissemination of the data must comply with the policies established and enforced by the agency.
 - d. Classification of Data: Clearly specify the data classification and its level of sensitivity (e.g., top secret, secret, confidential, restricted, unclassified, private, public, etc.), whether the data captured, stored, generated, or otherwise produced by a technology are considered public information, and whether it is subject to applicable public records act requests and under what circumstances.
 - e. Privacy Impact: Develop or adopt and use a formal privacy impact assessment (PIA)¹⁰ or similar agency privacy assessment on technology and the data it captures, stores, generates, or otherwise produces.
5. Operations
- a. Installation, Maintenance, and Support: Require regular maintenance, support, upgrades, calibration, and refreshes of a technology to ensure that it functions properly.
 - b. Deployment: Identify who is authorized to officially approve the deployment and use of a technology, and the conditions necessary for deployment and use, if applicable.
 - c. Training: Require training, and perhaps certification or other documented proficiency, if applicable, of all personnel who will be managing, maintaining, and/or using a technology. Training should also cover privacy protections on the use of the technology, and the impact and sanctions for potential violations.
 - d. Operational Use: Identify specific operational factors that must be addressed in deployment and use of a technology. (For example, for ALPR, the officer should i) verify that the system has correctly "read" the license plate characters; ii) verify the state of issue of the license plate; iii) verify that the "hot list" record that triggered the alert is still active in the state or NCIC stolen vehicle or other file, and confirm the

hit with the entering agency; and iv) recognize that the driver of the vehicle may not be the registered owner).

- e. Recordkeeping: Require recordkeeping practices that document all deployments of the technology, including who authorized the deployment; how, when, and where the technology was deployed; results of deployments; and any exceptions. Recordkeeping will support efforts to properly manage technology implementation, ensure compliance with agency policies, enable transparency of operations, enable appropriate auditing review, and help document business benefits realization.

6. Data Collection, Access, Use, and Retention

- a. Collection: Define what data will be collected, how data will be collected, the frequency of collection, how and where data will be stored, and under what authority and conditions the data may be purged, destroyed, or deleted in compliance with applicable local, state, and/or federal recordkeeping statutes and policies, court orders, etc. Identify the destruction/deletion methods to be used.
- b. Access and Use: Define what constitutes authorized use of data captured, stored, generated, or otherwise produced by a technology. Define who is authorized to approve access and use of the data, for what purposes and under what circumstances.
- c. Information Sharing: Specify whether data captured, stored, generated, or otherwise produced by a technology can be shared with other agencies, under what circumstances, how authorization is provided, how information that is shared is tracked/logged, how use is monitored, and how policy provisions (including privacy) will be managed and enforced. Any agency contributing and/or accessing shared information should be a signatory of a data sharing Memorandum of Understanding (MOU). Dissemination of any shared information should be governed by compliance with applicable state and federal laws, standards, agency privacy policies, and procedures as agreed in the MOU.
- d. Security: Define information systems security requirements of the technology and access to the data to ensure the integrity of the systems and confidentiality of the data. The security policy should address all state and federal mandated security policies, and clearly address procedures to be followed in the event of a loss, compromise, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of data, including how and when affected persons will be notified, and remedial and corrective actions to be taken.
- e. Data Retention and Use: Establish data retention schedules in accordance with state or federal law or policy, access privileges, purge,

and deletion criteria for all data captured, stored, generated, or otherwise produced by a technology. Agencies should consider differentiating between data that are part of an ongoing or continuing investigation and information that is gathered and retained without specific suspicion or direct investigative focus. Agencies may wish to limit the retention of general surveillance data. Empirical research assessing the performance of a technology may assist in determining an appropriate retention schedule.

7. Oversight, Evaluation, Auditing, and Enforcement
 - a. Oversight: Establish a reporting mechanism and a protocol to regularly monitor the use and deployment of a technology to ensure strategic alignment and assessment of policy compliance.
 - b. Evaluation: Regularly assess the overall performance of a technology so that it can i) identify whether a technology is performing effectively, ii) identify operational factors that may impact performance effectiveness and/or efficiency, iii) identify data quality issues, iv) assess the business value and calculate return on investment of a technology, and v) ensure proper technology refresh planning.
 - c. Auditing: Audit all access to data captured, stored, generated, or otherwise produced by a technology to ensure that only authorized users are accessing the data for legitimate and authorized purposes, and establish regular audit schedules.
 - d. Enforcement: Establish procedures for enforcement if users are suspected of being or have been found to be in noncompliance with agency policies.

Conclusion

Realizing the value that technology promises law enforcement can only be achieved through proper planning, implementation, training, deployment, use, and management of the technology and the information it provides. Like all resources and tools available to law enforcement, the use of new technologies must be carefully considered and managed. Agencies must clearly articulate their strategic goals for the technology, and this should be aligned with the broader strategic plans of the agency and safety needs of the public. Thorough and ongoing training is required to ensure that the technology performs effectively, and that users are well versed in the operational policies and procedures defined and enforced by the agency. Policies must be developed and strictly enforced to ensure the quality of the data, the security of the system, compliance with applicable laws and regulations, and the privacy of information gathered. Building robust auditing requirements into agency policies will help enforce proper use of the system, and reassure the public that their privacy interests are recognized and protected. The development of these policies is a proven way for executives to ensure they are taking full advantage of technology to assist in providing the best criminal justice services, while protecting the privacy, civil rights, and civil liberties of citizens.

¹ This Technology Policy Framework was developed by an ad-hoc committee of law enforcement executives and subject matter experts representing IACP Divisions, Committees, Sections, the IACP National Law Enforcement Policy Center, and other organizations and groups, including the Criminal Intelligence Coordinating Council, Major Cities Chiefs Association, National Sheriffs' Association, Major County Sheriffs' Association, Association of State Criminal Investigative Agencies, the Institute for Intergovernmental Research (IIR), the Integrated Justice Information Systems (IJIS) Institute, and federal partners.

² The American Civil Liberties Union (ACLU) recently released two reports addressing law enforcement technologies—ALPR and body-worn video. Both reports discuss the value of the technology to law enforcement operations and investigations, and both call for policies addressing deployment, operations, data retention, access, and sharing. Catherine Crump, *You are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, (New York: ACLU, July 2013), at <https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record>, and Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, a Win for All*, (New York: ACLU, October 2013), at <https://www.aclu.org/technology-and-liberty/police-body-mounted-cameras-right-policies-place-win-all>. Also see, Massachusetts Senate Bill S.1648, *An Act to Regulate the Use of Automatic License Plate Reader Systems*, Cynthia S. Creem, Sponsor, at <https://malegislature.gov/Bills/188/Senate/S1648>; Cynthia Stone Creem and Jonathan Hecht, "Check it, then chuck it," *The Boston Globe*, December 20, 2013, at <http://www.bostonglobe.com/opinion/2013/12/20/podium-license/R1tKQerVOYAPLW6VCKodGK/story.html>; Shawn Musgrave, "Boston Police halt license scanning program," *The Boston Globe*, December 14, 2013, at <http://www.bostonglobe.com/metro/2013/12/14/boston-police-suspend-use-high-tech-license-plate-readers-amid-privacy-concerns/B2hy9UizC7KzebnGyQ0JNM/story.html>; Ashley Luthern and Kevin Crowe, "Proposed Wisconsin bill would set rules for license-plate readers," *Milwaukee Journal Sentinel*, December 3, 2013, at <http://www.jsonline.com/news/milwaukee/proposed-wisconsin-bill-would-set-rules-for-license-plate-readers-b99155494z1-234324371.html>; Dash Coleman, "Tybee Island abandons license plate scanner plans," *Savannah Morning News*, December 3, 2013, at <http://savannahnow.com/news/2013-12-02/tybee-island-abandons-license-plate-scanner-plans#.UqCAy8RDuNO>; Kristian Foden-Vencil, "Portland police are collecting thousands of license plate numbers every day," *Portland Tribune*, December 3, 2013, at <http://portlandtribune.com/pt/9-news/2013130-portland-police-are-collecting-thousands-of-license-plate-numbers-every-day>; Alicia Petska, "City Council split over how to handle license plate reader concerns," *The News & Advance*, (Lynchburg, VA), November 12, 2013, at http://www.newsadvance.com/news/local/article_5327dc78-4c18-11e3-bc28-001a4bcf6878.html; Jonathan Oosting, "Proposal would regulate license plate readers in Michigan, limit data stored by police agencies," *MLive*, (Lansing, MI), September 9, 2013, at http://www.mlive.com/politics/index.ssf/2013/09/proposal_would_regulate_licens.html; Katrina Lamansky, "Iowa City moves to ban traffic cameras, drones, and license plate recognition," *WQAD*, June 5, 2013, at <http://wqad.com/2013/06/05/iowa-city-moves-to-ban-traffic-cameras-drones-and-license-plate-recognition/>; Richard M. Thompson, II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, (Washington, DC: Congressional Research Service, April 3, 2013), at <http://www.fas.org/sgp/crs/natsec/R42701.pdf>; Somini Sengupta, "Rise of Drones in U.S. Drives

Efforts to Limit Police Use,” *New York Times*, February 15, 2013, at <http://www.nytimes.com/2013/02/16/technology/rise-of-drones-in-us-spurs-efforts-to-limit-uses.html?pagewanted=all>; Stephanie K. Pell and Christopher Soghoian, “Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact,” *Berkeley Technology Law Journal*, Vol. 27, No. 1, pp. 117-196, (2012), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1845644; and Stephen Rushin, “The Legislative Response to Mass Police Surveillance,” *79 Brooklyn Law Review* 1, (2013), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344805. All accessed December 30, 2013.

³ Personally identifiable information (PII) has been defined as “...any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.” Government Accountability Office (GAO), *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, (Washington, D.C.: GAO, May 2008), p. 1, at <http://www.gao.gov/new.items/d08536.pdf>. McCallister, *et. al.*, define “linked” information as “information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual.” Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology*, (Gaithersburg, MD: NIST, April 2010), p. 2-1, at <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>. McCallister, *et. al.*, go on to describe *linked* and *linkable* information: “For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable.” *Id.* Both accessed December 30, 2013.

⁴ Justice Harlan first articulated a “constitutionally protected reasonable expectation of privacy” in *Katz v. United States*, 389 U.S. 347 (1967), at 361. Justice Harlan’s two-fold test is “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” *Id.* Many of the technologies being deployed by law enforcement capture information that is publicly exposed, such as digital photographs and video of people and vehicles, or vehicle license plates in public venues (i.e., on public streets, roadways, highways, and public parking lots), and there is little expectation of privacy. “A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” *United States v. Knotts*, 460 U.S. 276 (1983), at 281. Law enforcement is free to observe and even record information regarding a person’s or a vehicle’s movements in public venues. The U.S. Supreme Court, however, has ruled that the electronic compilation of otherwise publicly available but

difficult to obtain records alters the privacy interest implicated by disclosure of that compilation. *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989). Automation overwhelms what the Court referred to as the *practical obscurity* associated with manually collecting and concatenating the individual public records associated with a particular person into a comprehensive, longitudinal criminal history record. “[T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.” *Id.*, at p. 764. This has subsequently been referred to as the “mosaic theory” of the Fourth Amendment. *United States v. Maynard*, 615 F.3d 544 (D.C. Cir.) (2010). See also, Orin Kerr, “The Mosaic Theory of the Fourth Amendment,” *Michigan Law Review*, Vol. 111, p. 311, (2012), at <http://www.michiganlawreview.org/assets/pdfs/111/3/Kerr.pdf>. Accessed December 30, 2013.

⁵ These universal principles largely align with the Fair Information Practices (FIPs) first articulated in 1973 by the Department of Health, Education & Welfare (HEW). HEW, *Records, Computers and the Rights of Citizens*, July 1973, at <http://epic.org/privacy/hew1973report/default.html>. See, Robert Gellman, *Fair Information Practices: A Basic History*, Version 2.02, November 11, 2013, at <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>. Comparable principles have been articulated by various governmental agencies, including the U.S. Department of Homeland Security, (Hugo Teufel, III, *Privacy Policy Guidance Memorandum, Number: 2008-01*, (Washington, DC: DHS, December 29, 2008), pp. 3-4, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf); the Home Office in the United Kingdom (Home Office, *Surveillance Camera Code of Practice*, (London, UK; The Stationery Office, June 2013), pp 10-11, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf); and the Information and Privacy Commissioner of Ontario, Canada (Ann Cavoukian, *Guidelines for the Use of Video Surveillance Cameras in Public Places*, (Ontario, Canada: Information and Privacy Commissioner of Ontario, September 2007), pp. 5-6, at: http://www.ipc.on.ca/images/Resources/up-3video_e_sep07.pdf, and Ann Cavoukian, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigative Report (Privacy Investigation Report MC07-68)*, (Ontario, Canada: Information and Privacy Commissioner of Ontario, March 3, 2008), p 3, at: http://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf). Also see, National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, (The National Academies Press: Washington, D.C., 2008), at http://nap.edu/catalog.php?record_id=12452. All accessed December 30, 2013.

⁶ Law enforcement is not, for example, expected to notify the subjects of lawfully authorized wiretaps that their conversations are being monitored and/or recorded. These deployments, however, are typically subject to prior judicial review and authorization. See, e.g., *Katz v. United States*, 389 U.S. 347 (1967); *Berger v. New York*, 388 U.S. 41 (1967); *Title III, Omnibus Crime Control and Safe Streets Act of 1968*, 18 U.S.C. §§ 2510-2522, as amended by the *Electronic Communications Privacy Act of 1986*.

⁷ Federal Bureau of Investigation, *Criminal Justice Information Services (CJIS) Security Policy*, Version 5.2, August 9, 2013, CJISD-ITS-DOC-08140-5.2, at <http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>. Accessed December 30, 2013.

⁸ Additional guidance regarding safeguarding personally identifiable information can be found in the Office of Management and Budget (OMB) Data Breach notification policy (M-07-16), at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>, and state data breach notification laws available from the National Conference of State Legislatures, at <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>. Accessed December 30, 2013.

⁹ See, e.g., International Association of Chiefs of Police, *Model Policy: License Plate Readers*, August 2010 <http://iacppolice.ebiz.uapps.net/personifyebusiness/OnlineStore/ProductDetail/tabid/55/Default.aspx?ProductId=1223>; Paula T. Dow, Attorney General, *Directive No. 2010-5, Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data*, (Trenton, NJ: Office of the Attorney General, December 3, 2010), at <http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersI-120310.pdf>; Office of the Police Ombudsman, *2011 Annual Report: Attachment G: Body-Worn Video & Law Enforcement: An Overview of the Common Concerns Associated with Its Use*, (Spokane, WA: Spokane Police Ombudsman, February 20, 2012), at <http://www.spdombudsman.com/wp-content/uploads/2012/02/Attachment-G-Body-Camera-Report.pdf>; ACLU, *Model Policy: Mobile License Plate Reader (LPR) System*, (Des Moines, IA: ACLU, September 19, 2012), at <http://www.aclu-ia.org/iowa/wp-content/uploads/2012/09/Model-ALPR-Policy-for-Iowa-Law-Enforcement.pdf>. Many of these policy elements are also addressed in the National Research Council's report, *op. cit.*, specifically in chapter 2, "A Framework for Evaluating Information-Based Programs to Fight Terrorism or Serve Other Important National Goals," at pp. 44-67. All accessed December 30, 2013

¹⁰ A privacy impact assessment (PIA) is "a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme." Roger Clarke, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review*, 25, 2 (April 2009), pp. 125-135, at <http://www.rogerclarke.com/DV/PIAHist-08.html>. Law enforcement agencies should consider using the Global Advisory Committee's *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities* at <https://it.ojp.gov/gist/47/Guide-to-Conducting-Privacy-Impact-Assessments-for-State--Local--and-Tribal-Justice-Entities>. This resource leads policy developers through appropriate privacy risk assessment questions that evaluate the process through which PII is collected, stored, protected, shared, and managed by an electronic information system or online collection application. The IACP published *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, (Alexandria, VA: IACP, September 2009), at http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf. For a list of PIAs completed by the U.S. Department of Justice, see <http://www.justice.gov/opcl/pia.htm>; Department of Homeland Security, see <https://www.dhs.gov/privacy-office-privacy-impact-assessments-pia>. All accessed December 30, 2013.