Comprehensive Law Enforcement Review: The Importance of Technology in Policing

SUMMARY

Technology has become increasingly viewed by police and the public as important to many policing functions. In a rapidly changing and complex technological landscape, police agencies and leaders need to be able to identify, assess, and evaluate new technology for adoption and do so in ways that improve their effectiveness, efficiency, and evolution without infringing on individual rights. Unfortunately, technology use and acquisition can also have unintended consequences which may hinder its potential. Moreover, new technology requires training, maintenance, and management, and agencies must also use technology in ways that do not jeopardize their relationship with citizens.

The following summary focuses on 1) types of technologies used by law enforcement and their effectiveness, 2) challenges faced by law enforcement in implementing new technologies, 3) issues relating to governance, and 4) policies and privacy concerns.

1) CORE TECHNOLOGIES IN POLICING

Information technology

- Information technology (IT) is "the application of computers and telecommunications to store, retrieve, transmit and manipulate data,"[1] including record management systems (RMS), computer-aided dispatch systems (CAD), databases, and mobile computer and data terminals. IT systems that enable sharing of information across jurisdictions include the National Crime Information Center (NCIC), the Law Enforcement National Data Exchange (N-DEx), state fusion center systems, and LINX.[2] The use of information technology systems has become widespread; for instance, of local police departments serving populations of 25,000 or more, over 90 percent use in-field computers.[3]
- IT is also being used to facilitate identification through fingerprints and DNA. Automated fingerprint information systems (AFIS)[4] are searchable databases of digitized fingerprints, and the Combined DNA Index System (CODIS)[5] allows access to DNA profiles of convicted offenders and crime scenes.
- Studies assessing the effect of IT on policing have found mixed or contradictory results regarding the benefits of IT for officer productivity, case clearances, proactive policing, community policing, and problem solving, among other outcomes, though officers have generally been positive toward IT improvements.[6] Although IT can be used beneficially in policing, it is important to ensure that technical difficulties, time and resources to maintain systems, overambitious reporting requirements, possible reduced interaction with citizens, and the lack of focus on strategic uses do not overshadow these benefits.[7]
- Social media is used by law enforcement to solve and prevent crime, to interact with the community (seeking or providing information), to recruit, and to inform and communicate with staff.[8] While police use of social media may raise some privacy concerns, the key challenge is to find the time and

resources to process the vast amount of information available via social media and decide what is relevant.

Analytic technology

- Analytic technology "involves the use of large amounts of data and modern technology—along with a set of systematic methods and techniques that identify patterns and relationships between crime data and other relevant information sources—to assist police in criminal apprehension, crime and disorder reduction, crime prevention and evaluation."[9] Eighty-nine percent of agencies have personnel responsible for conducting crime analysis.[10]
- A prominent analytic technology is predictive policing, which uses analytic techniques to make statistical predictions that can "identify likely targets for police intervention."[11] Predictive policing is not a substitute for traditional or community-based policing, and to be successful, it must have sufficient support and resources.[12] Other areas that have benefited from analytic technology include hotspots policing, Compstat, investigative work, and problem-oriented policing tactics.[13]
- Research emphasizes that willingness to accept analytic technologies as part of strategic and tactical planning is key. Possible obstacles to effective use of analytic technologies include lack of resources, police culture, lack of training in proactivity or problem solving, and the low value placed on analysis by officers.[14] In some agencies, crime analysis is produced solely for police managers and short-term planning.[15]

Communication technology

- Radio is the primary means of communication in law enforcement agencies, with many agencies employing land mobile radio (LMR) technology, which enables police and sheriffs to have dedicated channels for their own use, priority access to other channels, and one-to-many group capability. LMR also gives law enforcement the ability to communicate device-to-device without a network infrastructure.
- Interoperability is a challenge to the use of communication technology and may depend on technology, policy, and spectrum use. Spectrum previously allocated for other purposes was redesignated for public safety use in 2012 and, thanks to the development of governance structures, is subject to spectrum planning and regional coordination.
- In the future, law enforcement communications will likely involve a combination of both LMR technology and broadband technology. Congress has authorized development of a nationwide public safety broadband network (FirstNet) that will use long term evolution (LTE).

Sensor and surveillance technology

- Some of the most influential and challenging policing technologies involve surveillance and sensory systems.
- Closed circuit televisions (CCTV) serve as deterrents to potential criminal activity and can provide law enforcement with real-time information. A recent review of the research on CCTVs found that

"CCTV has a modest but significant desirable effect on crime, is most effective in reducing crime in car parks," and "is most effective when targeted at vehicle crimes."[16]

- License plate readers (LPR) read vehicle license plates and compare these to a database of wanted offenders or stolen vehicles. Experimental studies regarding LPRs have found mixed impacts of the potential of LPR use to control or prevent crime.[17] Public support for LPRs has been found to vary based on the types of LPR application.[18]
- Body-worn cameras (BWC) are being adopted to improve evidence collection, strengthen officer performance and accountability, enhance agency transparency, and investigate and resolve complaints about officer-involved incidents. While the first randomized trial of BWCs found that officer shifts that were recorded were found to have approximately half as many incidents of use of force as those that were not recorded, similar studies did not find such significant results.[19]
- Unmanned aircraft systems (UAS) are increasing in popularity, although less is known about this technology than about other forms of surveillance. Work is currently underway to develop a guidebook for law enforcement use of UAS,[20] as well as an online database to capture flight-operations data from the use of small UAS (sUAS) in order to promote and enhance research on improving their safety and operational efficiency.[21]

Identification technology

- DNA analysis has become an increasingly common method of identification, most frequently used for sex crimes and other violent crimes, and its application to property crimes is expanding. Although limited, research suggests the use of DNA evidence helps police solve a large number of crimes and improve the likelihood of conviction in those cases.[22] However, according to a recent survey, "only 8 percent of local agencies have a local lab to conduct DNA testing, 88 percent send evidence to state labs for testing, and the remaining use federal, private, or other types of labs."[23]
- Backlogs of cases with untested forensic evidence result from limited financial resources and are an obstacle to effective use of DNA analysis.[24] Furthermore, rape kits may not always be sent to a lab for testing, which may be a result not only of financial constraints but also of policy.[25]
- With the development of new technology, both facial and iris scanning may soon be possible from mobile devices.[26] Facial recognition is controversial because it is one of the only biometrics that can collect data without the knowledge of the subject.[27]

Other technologies

- Body armor is now used in many police agencies. The Bureau of Justice Statistics reports that in 2007, 75 percent of local police departments and 73 percent of sheriff's departments required their officers to wear body armor at least part of the time. The International Association of Chiefs of Police (IACP)/DuPont Kevlar Survivors Club reports that more than 3,100 officers' lives have been saved by body armor since it was introduced into practice in 1975. Moreover, an officer who is not wearing body armor is more than three times more likely to suffer a fatal injury if shot in the torso than an officer who is wearing body armor.[28]
- Less-than-lethal technologies include conductive energy devices (CED) and oleoresin capsicum (OC) spray (pepper spray), which have been found to reduce rates of both officer and civilian injury.[29]

With regard to effectiveness, in a study that compared seven law enforcement agencies that use CEDs with six agencies that do not, researchers found a 70-percent decrease in officer injuries and a 40-percent decrease in suspect injures.[30]

2) CHALLENGES TO ACQUISITION, IMPLEMENTATION, AND USE

Combating cyber-crime

- Technology has opened the door for new areas of criminal activity, such as hacking and identity theft. While it is generally recognized that cyber-attacks pose a serious threat to law enforcement data systems, many agencies have not implemented strategies to mitigate that risk.[31]
- One major challenge to combating cyber-crime is jurisdiction. A cyber-crime that was perpetrated in one jurisdiction might have been initiated in another or even internationally. Likewise, the evidentiary data from a physical crime committed in one jurisdiction might be stored on a server in another.

Selecting technology

- Decision making about technology requires assessing potential risks, consequences, and outcomes of the acquisition and implementation of a given technology. In adopting a new technology, an agency must develop a detailed business plan and assess the return of investment for each given technology, as well as develop an understanding of potential risks of implementation.[32] In selecting a new technology, it is important that law enforcement agencies link the goals of the new technology with their agency's mission, style of policing, and the communities they serve.
- Law enforcement leaders may feel pressure to adopt new technologies from vendors, the public, or other agencies. Agencies may also be facing a particular crisis that prompts them to adopt a technology quickly without adequate time for review.[33] Although the National Institute of Justice funds studies in the impact of equipment and technology on policing, developing guides to assist agencies in making technology decisions, it often can take several years to complete these guides.
- Agencies often are unprepared for the unintended consequences that may accompany the acquisition of new technologies. Implementation of new technologies can cause disruptions to daily routines, lack of buy-in, and lack of understanding of the purpose and appropriate uses of the technologies. It also often raises questions regarding how the new technologies will impact the officers expectations, discretion, decision making, and accountability.[34]
- While considering the direct acquisition costs, many agencies fail to account for some of the ancillary costs associated with implementation. For instance, body-camera recording may yield a large number of inquiries from the public, which may take unanticipated man hours and legal counsel to address. Some agencies have mitigated some of these costs through cost sharing or regionalization efforts with partnering agencies.
- It is important that agencies establish the proper user and stakeholder input prior to the implementation of new technologies. Many agencies establish a planning committee responsible for the overall development of an acquisition plan with best planning committees incorporating

members from across the agency. Including all members of the agency encourages buy-in and helps identify potential user issues.[35]

3) CRITICAL GOVERNANCE ISSUES

- Managing the challenges brought by the adoption of new technology requires a robust governance structure that oversees the implementation plan, testing procedures, monitoring, training, technical assistance, audits, and evaluations.
- Training must not only focus on how to use the technology but also remind officers that they cannot rely on technology alone and neglect traditional police practices such as observation of their surroundings. In addition to training, technical assistance is often required to assist with problems and issues involved in technology implementation.
- Agencies should develop a reporting mechanism and procedure to regularly monitor how a given technology is being used and ensure it is in compliance with all policies.

4) POLICIES AND PRIVACY

- In order for technology to be successfully integrated into any agency, the proper policies and procedures must be issued prior to implementation. For instance, relevant policy considerations relating to BWCs include technology usage, data storage and retention, public access, and systems security.
- In implementing new technologies, it is of utmost importance that the public's privacy and civil liberties be protected.[36] When the public does not believe its privacy is being protected, a breakdown in community trust can occur. Agencies should consider ways to involve the public in discussions related to the protection of their privacy and civil liberties. With regard to BWCs, consideration must be given incidents with juveniles, undercover work, responding to calls at hospitals where Health Insurance Portability and Accountability Act (HIPAA) concerns are involved, and entering private homes. For their own privacy, officers should be given clear guidance on when they are permitted to turn off the camera.
- As noted earlier with the adoption of technology policies, stakeholder involvement is crucial in developing privacy guidelines. A simple one-size-fits-all approach is not appropriate, and police employees at all levels should be involved in discussions.

Conclusion

While technology is crucial to law enforcement, it is never a panacea. Its acquisition and use can have unintended consequences for both the organization and the community it serves, which may limit its potential. Considering the research behind core technologies and policies related to implementation and community concerns, as well as governance and management, are essential parts of strategizing about technology acquisition. Future areas of research should include an increased focus on the effectiveness of technology, not just the efficiency. There is also a need for additional research on the impacts of technology on crime control and prevention, as well as its effect on the police organization

itself. Other important topics for research are how technology improves or degrades citizen privacy and civil liberties and how it affects the public's attitudes toward the police and their perceptions of police legitimacy.

Further Readings

Agrawal, Manish, H.R. Rao, and G.L. Sanders. 2003. "The Impact of Mobile Computing Terminals in Police Work." *Journal of Organizational Computing and Electronic Commerce* 13(2):73–89. http://www.som.buffalo.edu/isinterface/papers/AgrawalRaoSandersJOCEC2003Police.pdf.

Cohen McCullough, Debra R. 2014. "Unmanned Aircraft Systems (UAS) Guidebook in Development." *Community Policing Dispatch* 7(8). http://cops.usdoj.gov/html/dispatch/08-2014/UAS_Guidebook_in_Development.asp.

Farrar, Tony, and Barak Ariel. 2013. *Self-Awareness to Being Watched and Socially-Desirable Behavior: A Field Experiment on the Effect of Body-Worn Cameras on Police Use-of-Force* (Washington, DC: The Police Foundation). http://www.policefoundation.org/sites/g/files/g798246/f/201303/The%20Effect%20of%20Body-Worn%20Cameras%20on%20Police%20Use-of-Force.pdf.

Harris, Kelly J., and William H. Romesburg. 2011. *Law Enforcement Tech Guide: How to Plan, Purchase, and Manage Technology (Successfully!)* (Washington, DC: Office of Community Oriented Policing Services). http://www.cops.usdoj.gov/Publications/lawenforcementtechguide.pdf.

Koper, Christopher S., Cynthia Lum, and James Willis. 2014. *Realizing the Potential of Technology in Policing: A Multi-Site Study of the Social, Organizational, and Behavioral Aspects of Implementing Police Technologies.* Final Report to the National Institute of Justice *(*Washington, DC: National Institute of Justice).

Police Executive Research Forum. 2013. *Social Media and Tactical Considerations for Law Enforcement* (Washington, DC: Office of Community Oriented Policing Services). http://ric-zai-inc.com/Publications/cops-p261-pub.pdf.

Stolling, Sharon, Shawn Barrett, and David Kurz. n.d. *Best Practices Guide for Acquisition of New Technology* (Alexandria, VA: International Association of Chiefs of Police). http://www.theiacp.org/portals/0/pdfs/BP-NewTechnology.pdf.

Taylor, Bruce, Daniel Woods, Bruce Kubu, Chris Koper, Bill Tegeler, Jason Cheney, et al. 2012. *Comparing Safety Outcomes in Police Use-Of- Force Cases for Law Enforcement Agencies That Have Deployed Conducted Energy Devices and A Matched Comparison Group That Have Not: A Quasi-Experimental Evaluation* (Washington, DC: Police Executive Research Forum). https://www.ncjrs.gov/pdffiles1/nij/grants/237965.pdf.

Welsh, Brandon C., and David P. Farrington. 2008. “Effects of Closed Circuit Television Surveillance on Crime,” *Campbell Systematic Reviews* 4(17). http://www.campbellcollaboration.org/lib/download/243/.

NOTES

[1] John Daintith, ed., "IT," in A Dictionary of Physics (Oxford University Press, 2009).

[2] "N-DEx-: The Leader in National Information Sharing," Federal Bureau of Investigation, accessed September 22, 2013, http://www.fbi.gov/about-us/cjis/n-dex;"Law Enforcement Information Exchange (LInX) and the Department of Defense Law Enforcement Defense Data Exchange (D-DEx)," Naval Criminal Investigative Service, accessed September 22, 2013, http://www.ncis.navy.mil/PI/LEIE/Pages/default.aspx.

[3] Christopher S. Koper, Cynthia Lum, and James Willis, *Realizing the Potential of Technology in Policing: A Multi-Site Study of the Social, Organizational, and Behavioral Aspects of Implementing Police Technologies—Final Report to the National Institute of Justice* (Washington, DC: National Institute of Justice, 2014).

[4] "Integrated Automated Fingerprint Identification System," Federal Bureau of Investigation, accessed January 10, 2015, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis.

[5] "Laboratory Services: Combined DNA Index System (CODIS)," Federal Bureau of Investigation, accessed January 10, 2015, http://www.fbi.gov/about-us/lab/biometric-analysis/codis.

[6] Manish Agrawal, H.R. Rao, and G.L. Sanders, "The Impact of Mobile Computing Terminals in Police Work," *Journal of Organizational Computing and Electronic Commerce* 13, no. 2 (2003): 73–89, http://www.som.buffalo.edu/isinterface/papers/AgrawalRaoSandersJOCEC2003Police.pdf; Mary Maureen Brown, "The Benefits and Costs of Information Technology Innovations: An Empirical Assessment of a Local Government Agency," *Public Performance and Management Review* 24, no. 4 (2001): 351–366, http://www.jstor.org/stable/3381224; Mary Maureen Brown and Jeffrey L. Brudney, "Achieving Advanced Electronic Government Services: Opposing Environmental Constraints," *Public Performance & Management Review* 28, no. 1 (2004): 96–113, http://www.jstor.org/stable/3381211; Janet Chan et al., *E-Policing: The Impact of Information Technology on Police Practices* (Brisbane, Australia: Queensland Criminal Justice Commission, 2001); Caran Colvin, *Evaluation of Innovative Technology: Implications for the Community Policing Roles of Law Enforcement Officers* (San Francisco: San Francisco State University, 2001); James N. Danziger and Kenneth L. Kraemer, "Computerized Data Systems and Productivity Among Professional Workers: The Case of Detectives," *Public Administration Review*, January/February 1985: 196–209, http://www.jstor.org/stable/3110149; Ralph E. Ioimo and Jay E. Aronson, "The Benefits of Police Field Mobile Computing Realized by Non-Patrol Sections of a Police Department," *International Journal of Police Science and Management* 5, no. 3 (2003): 195–206; Ralph E. Ioimo and Jay E. Aronson, "Police Field Mobile Computing: Applying the Theory of Task-Technology Fit," *Police Quarterly* 7, no. 4 (December 2004): 403–428, http://pqx.sagepub.com/content/7/4/403.full.pdf+html; Samuel Nunn, "How Capital Technologies Affect Municipal Service Outcomes: The Case of Police Mobile Digital Terminals and Stolen Vehicle Recoveries," *Journal of Policy Analysis and Management* 13, no. 3 (1994): 539–559; Samuel Nunn and Kenna Quinet, "Evaluating the Effects of Information Technology on Problem-Oriented Policing: If It Doesn't Fit, Must We Quit?" *Evaluation Review* 26, no. 1 (February 2002): 81–108, http://erx.sagepub.com/content/26/1/81.full.pdf; T.S. Palys, Ehor O. Boyanowsky, and Donald G.Dutton, "Mobile Data Access Terminals and their Implications for Policing," *Journal of Social Issues* 40, no. 3 (1984): 113–127; Bruce Rocheleau, "Evaluating Public Sector Information Systems: Satisfaction Versus Impact," *Evaluation and Program Planning* 16, no. 2 (1993): 119–129, doi: 10.1016/0149-7189(93)90023-2; Zaworski, "Assessing an Automated Information Sharing Technology in the Post '9-11' Era: Do Local Law Enforcement Officers Think It Meets Their Needs?" (doctoral dissertation, Florida International University, 2004).

[7] Koper et al., *Realizing the Potential of Technology* (see note 3).

[8] Police Executive Research Forum, *Social Media and Tactical Considerations for Law Enforcement* (Washington, DC: Office of Community Oriented Policing Services, 2013), http://ric-zai-inc.com/Publications/cops-p261-pub.pdf.

[9] Bruce Taylor and Rachel Boba, *The Integration of Crime Analysis into Patrol Work: A Guidebook* (Washington, DC: Office of Community Oriented Policing Services, 2011), 6, http://www.cops.usdoj.gov/Publications/e061120376_Integrating-Crime-Analysis-508.pdf.

[10] Taylor and Boba, *The Integration of Crime Analysis* (see note 9); Koper et al., *Realizing the Potential of Technology* (see note 3).

[11] Walter L. Perry et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (Washington, DC: RAND Corporation, 2013), xiii, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.
[12] *Predictive Policing: Forecasting Crime for Law Enforcement*, Research Brief (Washington, DC: RAND Corporation, 2013), http://www.rand.org/content/dam/rand/pubs/research_briefs/RB9700/RB9735/RAND_RB9735.pdf.
[13] David Weisburd and Cynthia Lum, "The Diffusion of Computerized Crime Mapping in Policing: Linking Research and Practice," *Police Practice and Research: An International Journal* 6, no. 5 (2005): 419–434, doi: 10.1080/15614260500433004; Bruce G. Taylor, Christopher S. Koper, and Daniel J. Woods, "A Randomized Control Trial of Different Policing Strategies at Hot Spots of Violent Crime," *Journal of Experimental Criminology* 7, no. 2 (June 2011): 149–181.
[14] Koper et al., *Potential of Technology in Policing* (see note 3); see also Nina Cope, "Intelligence Led Policing or Policing Led Intelligence? Integrating Volume Crime Analysis," *British Journal of Criminology* 44 (2004): 188–203; Gary Cordner and Elizabeth Biebel, "Problem-Oriented Policing in Practice," *Criminology & Public Policy* 4, no. 2 (2005): 155–180; Derek J. Paulson, "To Map or Not to Map? Assessing the Impact of Crime Maps on Police Officer Perception of Crime," *International Journal of Police Science and Management* 6, no. 1 (2004): 234–246.
[15] Christopher J. Harris, "Police and Soft Technology: How Information Technology Contributes to Police Decision Making" in *The New Technology of Crime, Law and Social Control*, eds. James M. Byrne and Donald J. Rebovich (Monsey, NY: Criminal Justice Press, 2007), 153–183; Timothy C. O'Shea and Keith Nicholls, "Police Crime Analysis: A Survey of U.S. Police Departments with 100 or More Sworn Personnel," *Police Practice and Research: An International Journal* 4, no. 3 (2003): 233–250; Taylor and Boba, *Integration of Crime Analysis* (see note 9)
[16] Brandon C. Welsh and David P. Farrington, "Effects of Closed Circuit Television Surveillance on Crime," *Campbell Systematic Reviews* 4, no. 17 (December 2008), 2, http://www.campbellcollaboration.org/lib/download/243/.
[17] Cynthia Lum et al., *License Plate Recognition Technology (LPR) Impact Evaluation and Community Assessment* (Fairfax, VA: George Mason Center for Evidence-Based Crime Policy, 2010), http://cebcp.org/wp-content/evidence-based-policing/LPR_FINAL.pdf; Cynthia Lum et al. "The Evidence-Based Policing Matrix," *Journal of Experimental Criminology* 7, no.1 (March 2011): 3–26; Christopher S. Koper, Bruce G. Taylor, and Bruce E. Kubu, *Law Enforcement Technology Needs Assessment: Future Technologies to Address the Operational Needs of Law Enforcement* (Washington, DC: Police Executive Research Forum, 2009), 22, http://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/law%20enforcement%20technology%20needs%20assessment%202009.pdf; see also Bruce G. Taylor, Christopher S. Koper, and Daniel Woods, "Combating Auto Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology" *Criminal Justice Review* 37, no. 1 (March 2012): 24–50, http://cjr.sagepub.com/content/37/1/24.full.pdf+htm.
[18] Linda Merola et al., "Community Support for License Plate Recognition," *Policing: An International Journal of Police Strategies and Management* 37, no. 1 (2014): 30–51. doi: 10.1108/PIJPSM-07-2012-0064; Linda Merola and Cynthia Lum, "Predicting Public Support for the Use of License Plate Recognition Technology by Police," *Police Practice and Research* 15, no. 5 (2014): 373–388, doi: 10.1080/15614263.2013.814906.
[19] Tony Farrar and Barak Ariel, *Self-Awareness to Being Watched and Socially-Desirable Behavior: A Field Experiment on the Effect of Body-Worn Cameras on Police Use-of-Force* (Washington, DC: The Police Foundation, 2013), http://www.policefoundation.org/sites/g/files/g798246/f/201303/The%20Effect%20of%20Body-Worn%20Cameras%20on%20Police%20Use-of-Force.pdf.
[20] Debra R. Cohen McCullough, "Unmanned Aircraft Systems (UAS) Guidebook in Development," *Community Policing Dispatch* 7, no. 8 (August 2014), http://cops.usdoj.gov/html/dispatch/08-2014/UAS_Guidebook_in_Development.asp; "Awards Related to: Online Flight and Incident Reporting System for Public Safety Use of Small Unmanned Aircraft Systems (sUAS)," accessed December 13, 2014, http://www.nij.gov/funding/awards/pages/awards-list.aspx?solicitationid=3793.
[21] "Awards Related to: Online Flight" (see note 21).
[22] "Using DNA to Solve Property Crimes," National Institute of Justice, accessed December 13, 2014, http://www.nij.gov/topics/forensics/evidence/dna/property-crime/Pages/solving-crimes.aspx.
[23] Koper, Lum, and Willis, "Realizing the Potential of Technology," (see note 3), 42.

[24] John K. Roman et al., *The DNA Field Experiment: Cost-Effectiveness Analysis of the Use of DNA in the Investigation of High-Volume Crimes* (Washington, DC: The Urban Institute, 2008), https://www.ncjrs.gov/pdffiles1/nij/grants/222318.pdf.

[25] "Untested Sexual Assault Evidence in Law Enforcement Custody," National Institute of Justice, accessed December 3, 2014, http://nij.gov/topics/forensics/lab-operations/evidence-backlogs/Pages/law-enforcement-sexual-assault.aspx.

[26] Sabrina A. Lochner, "Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology and Iris Scans," *Arizona Law Review* 55, no. 1 (2013): 201–233, http://www.arizonalawreview.org/pdf/55-1/55arizlrev201.pdf.

[27] Shimon Modi and Eugene H. Spafford, "Future Biometric Systems and Privacy," in *Privacy in America: Interdisciplinary Perspectives*, eds. William Aspray and Phillip Doty, 167–184 (Lanham, MD: Scarecrow Press, 2011).

[28] Tom LaTourrette, "The Life-Saving Effectiveness of Body Armor for Police Officers," *Journal of Occupational and Environmental Hygiene* 7, no. 10 (2010): 557–62.

[29] Bruce Taylor et al., *Comparing Safety Outcomes in Police Use-Of- Force Cases for Law Enforcement Agencies That Have Deployed Conducted Energy Devices and A Matched Comparison Group That Have Not: A Quasi-Experimental Evaluation* (Washington, DC: Police Executive Research Forum, 2009), https://www.ncjrs.gov/pdffiles1/nij/grants/237965.pdf; John M. MacDonald, Robert J. Kaminski, and Michael R. Smith, "The Effect of Less-Lethal Weapons on Injuries in Police Use-of-Force Events," *American Journal of Public Health* 99, no. 12 (2009) 2268–2274, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2775771/pdf/2268.pdf; Bruce G. Taylor and Daniel J. Woods, "Injuries to Officers and Suspects in Police Use-of-Force Cases: A Quasi-Experimental Evaluation," *Police Quarterly* 13, no. 3 (2010): 260–289, http://pqx.sagepub.com/content/13/3/260.full.pdf.

[30] Taylor et al., *Comparing Safety Outcomes* (see note 29).

[31] *Cyber Security: Addressing the Needs of Law Enforcement* (Alexandra, VA: International Association of Chiefs of Police, n.d.), http://www.theiacp.org/Portals/0/documents/pdfs/CyberSecurityBrief.pdf.

[32] Kelly J. Harris and William H. Romesburg, *Law Enforcement Tech Guide: How to Plan, Purchase, and Manage Technology (Successfully!)*, (Washington, DC: Office of Community Oriented Policing Services, 2011), http://www.cops.usdoj.gov/Publications/lawenforcementtechguide.pdf.

[33] David Weisburd and Cynthia Lum, "The Diffusion of Computerized Crime Mapping in Policing: Linking Research and Practice," *Police Practice and Research: An International Journal* 6, no. 5 (2005): 419–434, doi: 10.1080/15614260500433004.

[34] Koper et al., *Potential of Technology in Policing* (see note 3).

[35] Sharon Stolting, Shawn Barrett, and David Kurz, *Best Practices Guide for Acquisition of New Technology* (Alexandria, VA: International Association of Chiefs of Police, n.d.), http://www.theiacp.org/portals/0/pdfs/BP-NewTechnology.pdf.

[36] *IACP Technology Policy Framework* (Alexandria, VA: International Association of Chiefs of Police, 2014), http://www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf.