



Law and justice 2020

2020 sees law enforcement using innovative new methods and technologies to protect public safety and rehabilitate offenders. Mobile computing and electronic monitoring enable virtual incarceration. Gamified web and mobile interfaces deliver jobs training, connections, and rehabilitation services. Data analytics ensure that interventions are tailored to offenders' profiles. As crime becomes more sophisticated, so does policing: Drones act as eyes in the sky, while officers on the ground use wearable computing, facial recognition software, and predictive video. The fight against cyber- and biocrime shifts from a purely national responsibility to an increasingly important focus on local law enforcement.

Out-of-the-box justice

Big data for micro-tailored interventions

Justice centers leverage “big data” during pre-trial hearings, sentencing, and parole hearings to determine the most appropriate candidates for virtual incarceration. These tools help judges select effective combinations of interventions specifically targeted for individual needs and risks. Analytics and predictive modeling—some from novel sources such as facial coding software, which tracks facial expressions to reveal emotions and predict future behavior—reduce the individual and system-level risk of virtually incarcerating offenders.

The Risk Assessment and Sentencing Tool (RAST)—a sophisticated data analytics engine—helps classify offenders as low, medium, and high risk, and makes targeted sentencing recommendations.

Winning the “reform” game

Gamified interfaces on web and mobile apps allow offenders to connect and stay engaged with remote training and meetings. Offenders earn points tied to rewards for making check-ins, staying out of high-risk zones, and completing pro-social behavioral exercises. Game elements allow

offenders to see their progress and break up large goals into smaller, more manageable tasks, making the reform process engaging and achievable. Case managers benefit from dashboards offering features such as interactive maps that allow them to see their charges' movement patterns and behavioral data in real time.

Justice restored: A dual approach to sentencing

Sentencing increasingly incorporates interactions such as victim-offender mediation, family-group conferences, and community restorative boards, which use trained citizens to confront offenders with the consequences of their actions and discuss possible reparations. Benefits include less traumatic stress and related costs for victims and a lower rate of recidivism. Restorative justice programs, enabled by technology, facilitate connections between victims and offenders to create virtuous feedback loops that provide closure and the ability to move on for victims and offenders alike.

Goldman Sachs invested \$9.6 million in the Adolescent Behavioral Learning Experience program, a social impact bond that seeks to bring down the number of young offenders going back to prison on Riker's Island.

Justice "markets"

Public-private exchanges and full-fledged markets in recidivism reduction and preventative services become ubiquitous, addressing the factors that contribute to criminal behavior (drug dependence, mental health problems, lack of financial and peer support). Open markets—where buyers include governments, foundations, and offender families, and sellers include nonprofits, social enterprises, companies, and other governments—are complemented by government-led solutions.

Next-generation policing

Pervasive policing

Real-time intelligence and police demand-matching become so exact and quick that would-be offenders are deterred by a sense of "justice everywhere." Analytics such as crime mapping, geospatial prediction, data mining, and social network analysis, as well as omnipresent sensor networks and, ultimately, driverless cars that allow officers to operate as data mechanics in a mobile laboratory, coalesce to deliver not just faster response times when crimes occur but the intelligence needed to thwart crimes before they happen.

The PredPol tool, piloted in Los Angeles and Santa Cruz police departments, helps develop probabilities of future crime events. In a pilot in Los Angeles' Foothill division, PredPol helped reduce property crimes by 13 percent within four months.

Drone police

Unmanned aerial vehicles and ground-based drones supplement human patrols in almost every stage of policing. During recon, UAVs provide cheaper, more scalable alternatives to police helicopters, gathering and transmitting data in lieu of beat cops. Remote-controlled drones represent the front line in high-risk situations such as stand-offs and bomb threats, saving lives and tens of thousands of taxpayer dollars in manpower and cleanup costs.

Human robocops

Manpower meets computing power. Equipped with an augmented reality app, the camera on a cop's mobile device becomes as indispensable as a sidearm or handcuffs. Data-overlaid video feeds on handhelds, cruiser windshields, and wearable computers such as Google Glass give officers access to real-time language translation, cultural or biometric maps, floor plans, and more, as well as instant identification capabilities via facial recognition software. Bolstered by powerful GPS and crowd-tracking capacities, losing a suspect now happens infrequently. Patrol patterns become organic and unpredictable as analytics inside patrol cars route officers to areas of high risk.

Facial-recognition ID systems

Agents match faces-in-crowd photos and closed-circuit television images against the criminal database. In an instant, agents can identify subjects and their records, and tap real-time data feeds if the subject is serving a virtual incarceration sentence.

Crime fighting via predictive video

Cities' closed-circuit television networks, both public and private, become an integral part of proactive crime fighting. While CCTV cameras have been used in subways and streets to identify crime in a retroactive capacity for years, video-analytics software now added to feeds detects peculiar crowd and traffic movements and suspicious vehicles, bags, or people, transforming visual data into real-time intelligence.

Singapore's Safe City Test Bed project applies predictive analytics to video feeds to detect which street incidents—crowd and traffic movements—could cause a threat to public safety.

Crime prevention officers

As police efforts shift from reacting to crime to stopping it before it occurs, neighborhood police officers are recast as crime prevention officers. As the UK's Policy Exchange envisions it, these CPOs have much more autonomy than traditional officers and are held directly responsible for crime prevention in their areas. CPOs are equipped with body cameras to collect evidence and protect them from false claims, and meet with commanding officers regularly to review data on their performance. CPOs also play a larger role in the procurement process, testing the latest tools and providing vital feedback before their departments green-light new technology. Creating this new cadre of cops requires a significant change in hiring practices, as CPOs are vetted on the basis of their ability to absorb information quickly and master the newest technologies with ease.

Crowdsourced crime prevention

Real-time crowdsourcing of data on crime (incidence, degree, and nature) helps create large databases that can be used to identify areas meriting greater security. Through social media, citizens play a greater role in calling attention to specific issues and identifying and tracking down perpetrators.

The London Metropolitan Police, during the 2011 riots, crowdsourced the identities of 2,880 suspects using a smartphone application. The police asked citizens to download the Face Watch ID app and help identify the persons through images taken from CCTV footage. If an image was known to them, citizens entered the name or address of the person, which was sent to the police immediately and confidentially.

Upgrading cyber security

Innovation hubs to fight cyber crime

By 2020, much of the world's crime is committed through the Internet. Advanced cyber security becomes a necessity—and a huge economic opportunity for innovative problem-solvers and governments willing to collaborate with them. These public-private collaborations look like technology campuses, featuring incubators and “lean” security startups that employ white-hat hackers and emphasize rapid testing and learning, integrating the latest trends into daily police activities.

The Hague Security Delta, a partnership of companies, governments, and research institutions, applies Silicon Valley's ecosystem approach to cyber security.

The US Department of Defense faces 10 million cyber-attacks. per day

Interagency security initiatives

Because of the urgency of the challenge and the need for expertise and economy, different arms of government join forces to fight cybercrime. Governments follow the lead of the Netherlands, which has launched a National Cyber Security Center, a Center of Information Security and Privacy, and a center for municipal cyber security.

Cyber security goes horizontal

Cyber security adopts cybercrime's networked, decentralized structure as rigid top-down lines between international, national, and local jurisdictions dissolve. Security leans heavily on technology, lightweight solutions, and international collaboration, characteristics defining a new cadre of global enforcement officers. These GEOs, created at the federal level, can bypass international jurisdictions and seamlessly join foreign teams to bring global cybercriminals to justice.

"Biocrime" demands bio security

The world sees a spike in a new form of crime, biocrime, as advanced, genetically targeted weapons and DNA-related identity theft insidiously trail the personalized medicine and molecular therapies movement. In response, governments and private genetics companies engage in a global effort to concentrate DNA information in central, secure databases.

Transparency algorithms to identify cyber perpetrators

One of the biggest challenges of fighting cybercrime is identifying the perpetrator. Police team with academia to build arsenals of algorithms designed to unmask international cybercriminals. From intrusion software to big data correlation, cyber cops now have a range of tools to connect pieces of data with individuals. These algorithms represent some of the core activities at innovation hubs and cybercrime centers. Powerful cloud analytics help agents predict future cybercrime activity. The latter technology requires extensive international cooperation as cloud services and storage providers must agree to participate.

Online national IDs

As a result of the need for stronger means of online authentication, companies and citizens increasingly rely on government-standardized electronic IDs to interact with all parts of government and commerce. Such identification becomes a de facto requirement for all online services from government, healthcare providers, and multinational companies.

Sources

Deloitte deeper dives

Alan Holden and Kara Shuler, Beyond the bars: A new model of virtual incarceration for low-risk offenders, Deloitte University Press, March 4, 2013, <http://dupress.com/articles/beyond-the-bars/>.

Anesa Diaz-Uda and Joe Leinbach, The power of zoom: Transforming government through location intelligence, Deloitte University Press, February 13, 2013, <http://dupress.com/articles/the-power-of-zoom/>.

Christian Doolin, Alan Holden, and Vignon Zinsou, Augmented government: Transforming government services through augmented reality, Deloitte, June 6, 2013, http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/Federal/us_fed_augmented_government_060613.pdf.

Deloitte, The cyber savvy agency, http://www.deloitte.com/view/en_US/us/Industries/US-federal-government/federal-focus/cyber/fa9a0026d3ff6210Vgn-VCM200000bb42f00aRCRD.htm.

Shehryar Khan and Evangeline Marzec, Tech Tends 2014: Wearable, Deloitte University Press, February 21, 2014, <http://dupress.com/articles/2014-tech-trends-wearables/>.

Vikram Mahidhar, David Schatsky, and Kelly Bissell, Cyber crime fighting, Deloitte University Press, June 27, 2013, <http://dupress.com/articles/cyber-crime-fighting/>

William Eggers and Joshua Jaffe, Gov on the Go: Boosting public sector productivity by going mobile, Deloitte University Press, February 18, 2013, <http://dupress.com/articles/gov-on-the-go/>.

Other sources

Addy Dugdale, "Police use facial-recognition technology on driver's licenses and other IDs to aid crime solving," Fast Company, June 17, 2013, <http://www.fastcompany.com/3013080/fast-feed/police-use-facial-recognition-technology-on-drivers-licenses-and-other-ids-to-aid->.

Carol Hedderman, Darrick Joliffe, Sion Cave et al., Peterborough Social Impact Bond: An independent assessment, UK Ministry of Justice Research, May 2012, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/217392/peterborough-social-impact-bond-assessment.pdf.

Darwin Bond-Graham and Ali Winston, "All tomorrow's crimes: The future of policing looks a lot like good branding," SF Weekly, October 30, 2013, <http://www.sfweekly.com/2013-10-30/news/predpol-sfpd-predictive-policing-compstat-lapd/>.

Edward Boyd and David Skelton, "Policing 2020: What kind of police service do we want in 2020?," Policy Exchange, December 12, 2012, <http://www.policyexchange.org.uk/publications/category/item/policing-2020-what-kind-of-police-service-do-we-want-in-2020>.

Electronic Privacy Information Center, "National strategy for trusted identities," <http://epic.org/privacy/nstic.html>.

Ger Daly, "Embracing the police force of the future," CNN, September 19, 2013, <http://edition.cnn.com/2013/09/18/tech/innovation/police-future-technology/>.

Goldman Sachs, Mayor Bloomberg, deputy mayor Gibbs and corrections commissioner Schriro announce nation's first social impact bond program, August 2, 2012, <http://www.goldmansachs.com/what-we-do/investing-and-lending/urban-investments/case-studies/social-impact-bond-pdf.pdf>.

Haque Security Delta, "Building cyber resilient cities," www.hcss.nl/reports/download/147/2428/.

Maggie Overfelt, "Terminator Town USA: Rise of the everyday robot," CNBC, September 13, 2013, <http://www.cnn.com/id/101030655>.

Marc Goodman and Andrew Hessel, "The bio-crime prophecy: DNA hacking the biggest opportunity since cyber-attacks," Wired, May 28, 2013, <http://www.wired.co.uk/magazine/archive/2013/06/feature-bio-crime/the-bio-crime-prophecy>.

Mikko Hypponen, "Fighting viruses, defending the net," TED, July 2011, http://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net?language=en.

National Cyber Security Center, Netherlands Ministry of Security and Justice, "National Cyber Security Strategy," <https://www.ncsc.nl/english/organisation/about-the-ncsc/background.html>.

Paul Marks, "Augmented reality iPhone helps police track suspects," New Scientist, February 21, 2011, http://www.newscientist.com/article/dn20153-augmented-reality-iphone-helps-police-track-suspects.html#.Uz0F3_kaaT9.

Predpol, "About," <http://www.predpol.com/about/>.

Shako Liu, That's suspicious behavior: Can crowdsourcing prevent crime near USC?, Crowd Sourcing, September 18, 2012, <http://www.crowdsourcing.org/article/thats-suspicious-behavior-can-crowdsourcing-prevent-crime-near-usc/19261>.

Thomas J. Cowper and Michael E. Buerger, Improving our view of the world: Police and augmented reality technology, Federal Bureau of Investigation, <http://www.fbi.gov/stats-services/publications/police-augmented-reality-technology-pdf>.

Tom Brewster, "How the UK's new cyber cops will wage war on the dark web," Wired, October 21, 2013, <http://www.wired.co.uk/news/archive/2013-10/21/cyber-crime-dark-web>.

Zachary Fryer-Briggs, "U.S. military goes on cyber offensive," Defense News, March 24, 2012, <http://www.defensenews.com/article/20120324/DE-FREG02/303240001/U-S-Military-Goes-Cyber-Offensive/>.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2014 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited