4

SURVEILLANCE TECHNOLOGY CHALLENGES POLITICAL CULTURE OF DEMOCRATIC STATES

Inez Miyamoto

The debate about the adoption of surveillance technologies by different systems of government is already over: both autocratic and democratic states use surveillance technologies. Autocratic states, such as China, Russia, and Saudi Arabia, embrace surveillance technologies to control their citizens.[1] They find the surveillance technologies to be effective because once citizens know that their communications and movements are being monitored, they change their behavior without any government intervention.[2] In contrast, democratic states use surveillance technologies to improve public safety and national security but struggle with balancing state and citizen interests. Accordingly, this article centers on the use of surveillance technologies by democratic states against their citizens. The use of surveillance technologies against citizens challenges the existing political culture of democratic states—the fundamental beliefs, values, and norms that have long defined them. In other words, surveillance technologies conflict with the agreement between democratic governments and their citizens for privacy and civil liberty protections. Democratic states must act now to resolve this debate because the unprecedented speed of technological change is generating a gap between how these states and their citizens understand their own political culture.

Democratic states use surveillance technologies to facilitate governance through social control. Torin Monahan explains democratic surveillance as "intentionally harnessing the control functions of surveillance for social ends of fairness, justice, and equality."[3] In theory, democratic states

counterbalance social control through citizen participation and democratic controls (e.g., oversight, transparency, and public accountability). In practice, citizen participation and democratic controls can be effective in counteracting privacy-invasive surveillance, but they tend to be reactive and slow to respond. Meanwhile, recent advancements in surveillance technologies provide democratic states with unprecedented power to identify, track, and analyze their citizens in real-time. In other words, digital mass surveillance can become the norm for democratic states if allowed to go unchecked.

This chapter examines the struggle that democratic states are having to resolve the tension between political culture and surveillance technologies; tension often displayed in differences between policymakers, security practitioners and civil society members. The first section examines three U.S. case studies to show how surveillance technology is creating friction between the government and civil society. The second section analyzes the roles of the private sector and the state to identify the drivers contributing to the tension with political culture. The third section imagines future technologies and their impact on the current debate. The final section concludes with recommendations for resolving the political culture gap between governments and their citizens.

Debating Aspects of Surveillance Through Case Studies

This section examines three U.S. case studies to understand how surveillance technologies can undermine democratic political culture. Each of the case studies illuminates how free media and civic groups play an important role in identifying violations of civil liberties and ensuring public accountability.

Social Media and Facial Recognition

In 2016, the American Civil Liberties Union (ACLU) of Northern California sounded the alarm that law enforcement was accessing social media intelligence to monitor social protests. By seeking public records to determine how law enforcement was using social media monitoring, the ACLU obtained the marketing materials of the social media monitoring company Geofeedia, which touted the Baltimore Police Department's successful use of its product.[4] Specifically, after using Geofeedia's product to obtain

social media photos of protesters, the Baltimore Police Department ran the photos through facial recognition technology to identify and arrest individuals with outstanding warrants.[5]

Upon learning how Geofeedia was using the social media feeds, social media companies (i.e., Facebook, Instagram, and Twitter) suspended Geofeedia's access citing policies prohibiting their data from being used for surveillance activities. Without the social media feeds, Geofeedia could not manually collect social media posts to provide a real-time view of multiple social media feeds. The impact on Geofeedia was significant, causing layoffs and a business model shift to social media marketing and management.[6]

This is not an issue of law enforcement using social media platforms, which is publicly available information. When individuals post a public comment or picture on a social media platform, they want the public to see their content and are explicitly giving up their right to privacy. Since the comment or photo is open for the world to see, law enforcement is permitted to view and use public content. To prevent public access, individuals can increase their privacy settings so that only their followers can see their posts and photos. In this instance, law enforcement is required to obtain a court order to access the individuals' information.

Instead, the key issue here was law enforcement using a social media monitoring tool without a clear investigative purpose. Since individuals had a right to participate in a social protest, law enforcement had no investigative predication to identify individuals, let alone to check for outstanding warrants. Had there been a crime committed during the protest, then law enforcement could have justification to use facial recognition software in order to identify a suspect.

The underlying problem with Baltimore Police Department's use of Geofeedia's tool was its lack of transparency. When the department's use

Facial recognition technology is used to identify people using biometrics through biological or behavioral characteristics and consists of two processes. First, in the enrollment process, a person's facial features are mathematically mapped as facial landmarks into a template and saved in a database of known individuals. Second, in the matching process, a photo of an unknown person is processed using facial technology and compared against a database of known individuals. Factors affecting the accuracy of matches include the technology (e.g., the way facial landmarks are calculated) and the quality of a photo image.

of the tool was revealed, it eroded public trust already strained by the police brutality incident which had sparked the protest. By being open about the social media tool and having clear policies on use of surveillance technologies, the Baltimore Police Department could have eased public concerns.

Website Scraping and Facial Recognition

In January 2020, the *New York Times* published a report about Clearview AI's invasive facial recognition product, which was being used by law enforcement to identify individuals. Clearview AI sells access to a platform which identifies an individual by using a facial recognition search against a database containing three billion images. After the news article was published, private technology companies (e.g., Facebook, Twitter, Venmo, and Google) issued cease and desist letters to Clearview AI citing violations to their terms of service.[7] In response to the letters, Clearview AI claimed it had a right to publicly available information, likening its business to a search engine pulling information from different websites.[8]

In order to create a database of three billion images, Clearview AI extracted images from open websites using a process called website scraping, which is legal. In September 2019, the U.S. Court of Appeals for the 9th Circuit ruled that it is not illegal to scrape publicly accessible websites.[9] This ruling is currently being appealed; if the ruling is overturned, it could widen Clearview AI's legal troubles beyond the lawsuits it is facing in California, Illinois, and Vermont.

In February 2020, Clearview AI disclosed that an intruder stole its client list along with details about each client.[10] At the same time, *BuzzFeed News* revealed that it obtained internal Clearview AI documents from an undisclosed source, which included Clearview AI's client list of 2,228 organizations and individuals. The size of the client list is somewhat misleading as a majority of the clients were using free-trial licenses rather than a paid subscription. Clients with paid subscriptions included many federal government agencies (e.g., U.S. Immigration and Customs Enforcement

Web scraping is the process of collecting data from websites. The process is automated by using web crawlers, which are programs or scripts designed to browse and lift information from the World Wide Web. Other terms for web scraping include web data extraction and web harvesting.

and U.S. Secret Service) and local law enforcement agencies.[11]

Biometric technology is used to identify or authenticate by using the biological attributes of individuals. Individuals can be identified using physiological biometrics (e.g., retina, vein, or fingerprint) or behavioral biometrics (e.g., gait, signature, or keystrokes). Facial recognition and fingerprint recognition are examples of biometrics.

In this case study, law enforcement used a private-sector database to identify individuals, whereas in the Geofeedia case law enforcement used a government database. Law enforcement agencies traditionally rely on government databases for criminal identification, but an individual may not be in government databases. Clearview AI's technology provided an alternative for identifying individuals through open-source images. According to Clearview AI, law enforcement's use of its product does not violate any federal and state privacy or biometrics laws if it is used for its intended purpose and is not the sole basis for an arrest.[12] However, Clearview AI's database was controversial because the company violated individuals' rights: it never received the informed consent of the individuals owning the images or allowed individuals to opt out of its database.

Video Surveillance

There are two types of video surveillance commonly used: stationary and aerial video surveillance cameras. The first type involves the use of stationary cameras mounted at key locations. The second type involves the use of aerial craft mounted with cameras, which can be manned or unmanned. As an illustration, the military developed wide-area surveillance technology for use on a battlefield, but now law enforcement is using it for policing, border control, and wildlife protection.

In 2016 the Baltimore Police Department contracted with a wide-area surveillance company called Persistent Surveillance Systems. Over a period of several months, the company collected over 300 hours of surveillance video using aerial craft. After the plane downloaded the images onto a server hard drive, police could access the imagery to solve crimes. The video resolution did not allow for the identification of individuals or vehicles, but it was good enough to follow objects over time.[13]

After the program ended, *Bloomberg News* published an article revealing the Baltimore Police Department's use of wide-area surveillance tech-

nology. Public officials had no idea of the existence of the program because normal public spending oversight mechanisms were circumvented. Instead of using public funding, the police used a private donation from the Laura and John Arnold Foundation. The Foundation, which supports evidence-based policing solutions, had a prior agreement with Persistent Surveillance Systems to fund the project if the company could find a police department to use the technology.[14]

The Baltimore Police Department did not violate the law because U.S. laws allow for aerial surveillance without a warrant as long as the technology is publicly accessible.[15] The police wanted the technology because most of Baltimore's homicides occur in outdoor public spaces.[16] Since the camera resolution does not allow for visual identification of individuals or vehicles, there is even less of an invasion of privacy. Nevertheless, the department lost the public's trust because it was not transparent: it did not provide public notification, go through the normal procurement review, or publish its wide-area surveillance policy.

Despite all of the controversy, in 2019, Persistent Surveillance Systems solicited the Baltimore Police Department for a long-term contract. The three-year contract for US$6.6 million, which was funded again by the Laura and John Arnold Foundation, involved three planes, and covered 32-square miles. Persistent Surveillance Systems also disclosed its privacy program, limiting the resolution of images to prevent the identification of individuals.[17] Since the Baltimore Police Department was transparent and involved the public, in April 2020, the city of Baltimore approved the contract.

The Roles of the Private Sector and the State

Although the surveillance technologies used in the case studies were not illegal, they undermined democratic political culture because they went against the beliefs, values, and norms of what citizens expected of their government. Two insights emerge from the case studies. First, governments are highly reliant on private-sector surveillance technology because they do not organically possess these technologies or skills. Second, there is a lack of legal and policy frameworks at the national level to guide local governments in balancing citizen privacy and government surveillance. This section analyzes the roles of the private sector and state in surveillance technology use and explains the drivers contributing to the tension in democratic states' political culture.

Role of the Private Sector

Surveillance technology growth is now being driven by the private sector. The United Nations (UN) concluded: "Digital surveillance is no longer the preserve of countries that enjoy the resources to conduct mass and targeted surveillance based on in-house tools. Private industry has stepped in, unsupervised and with something close to impunity."[18] The private sector, in its pursuit for profit, indiscriminately sells surveillance tools around the world. For example, although Chinese companies are the largest global suppliers of surveillance technologies empowered by artificial intelligence (AI), private companies from democratic states, such as the United States, France, Germany, Israel, South Korea, United Kingdom, and Japan, are also selling surveillance technologies to both democracies and autocracies.[19]

International organizations are calling for regulations to monitor and control the export of surveillance technologies, since repressive governments use them to facilitate human rights abuses. For example, in 2014 the European Union (EU) banned the export of information communication and technology (ICT) to governments censoring information or conducting mass surveillance. And, in 2016, the European Commission specified the ICT for export control so that EU sales and exports of these technologies could be monitored.[20] In spite of having regulations, export-control laws are ineffective because they lack enforcement measures to address human rights violations and do not stop the use of the technologies.[21] Furthermore, since surveillance technologies are now widely available in many products, it would be impossible to regulate all of the technologies.

There is also a growing problem with the private sector's involvement in surveillance technologies: the surveillance limitations placed on the government do not always apply to the private sector. When the private sector closely works with government, the boundaries become unclear.[22] As discussed in the case studies, law enforcement leverages private sector

Artificial intelligence (AI) is the simulation of human intelligence in machines by using software. There are three general types of AI: artificial narrow intelligence, artificial general intelligence, artificial super intelligence. Artificial narrow intelligence involves systems performing defined tasks and is found in commercialized applications, such as Siri or facial recognition technology. Researchers are striving to achieve artificial general intelligence, which occurs when systems perform human-like thinking, and artificial super intelligence, which occurs when systems become more capable than humans.

technology to fight crime. In the future as more data becomes available, law enforcement may need to outsource the digital analysis and investigation to the private sector; thereby, the private sector becomes an extension of the government. This could be problematic if a private company were to sell a service to law enforcement and then unknowingly sell the same service to a criminal organization, or if the private company were to use the insider policing information for profit.

Private companies can also use surveillance technologies to monitor their customers without transparency or individual consent (i.e., in states without comprehensive privacy and security laws). While the biometric data compiled from facial, voice, and body-language analysis support the marketing and/or product sales of private companies, the data is extremely invasive (e.g., some data can be used to determine health, disease, or personality) and raises ethical and privacy concerns.[23] Another problem with surveillance data is the data retention period. Unless there are regulations or laws, the private sector is not required to follow the beliefs, values, or norms of a democratic state.

As the driver of surveillance technology growth, the private sector can increase trust with the government and civil society by self-regulating their use and sales of surveillance technology. Specifically, private companies that sell surveillance technologies can promote governance policies to address ethical and privacy concerns, establish an ethics board, and provide an annual transparency report. The private sector can also engage with civil society organizations to address the ethical problems raised by surveillance technologies. As an illustration, the Partnership on AI is one such organization working to increase AI dialogue among for-profit companies and academic and research institutions.[24]

Role of the State

At the international level, states should engage in multilateral discourse to avert the potentially dangerous side effects of surveillance technologies to democratic political culture. In reality, states will find it difficult to reach consensus and to establish international norms and standards for two reasons. Firstly, surveillance technologies are dual-use—having both civilian and defense applications—so they are the sources of geopolitical competition. States are unwilling to restrict their development of dual-use technologies because they are accelerators of economic growth and national defense advantage.[25] Secondly, technological innovation is accel-

erating faster than global governance. According to the Office of the Director of National Intelligence, "technological change will continue to far outpace the ability of states, agencies and international organizations to set standards, policies, regulations, and norms."[26] Under those circumstances, the gap between technology and governance will only widen.

Nevertheless, there are other ways states can work collaboratively toward global norms and standards in areas such as human rights, ethics, and safety. International organizations, such as the North Atlantic Treaty Organization (NATO) and International Committee of the Red Cross, provide opportunities to identify common values and approaches for increasing trust in surveillance technologies. In a like manner, while the Organisation for Economic Co-operation and Development (OECD) Principles on AI are non-binding, they establish political commitment to promote AI that is trustworthy and respects human rights and democratic values.[27] Additionally, the World Economic Forum has an initiative to bringing private and public stakeholders together to design and test policy frameworks for technologies such as AI, machine learning, and facial recognition.[28] These types of initiatives are the first steps toward global cooperation.

At the domestic level, states should consider establishing comprehensive security and privacy laws and engaging in dialogue with their citizens about surveillance technologies. First, the EU's General Data Protection Regulation (GDPR) is considered to be one of the strictest and most comprehensive laws for privacy and security.[29] The regulation was passed in 2014 when surveillance technologies were not as advanced as they are today. Consequently, critics are calling for GDPR regulatory reforms because it hinders the development and use of AI by placing limitations on the collection and sharing of personal data.[30] In addition, although the GDPR limits live facial recognition by mandating individual consent, it also specifies exceptions for law enforcement use, personal use, and situations where a person cannot be identified.[31] Therefore, while the GDPR is a proven framework that can be used to build a comprehensive privacy and security law, the GDPR should be expanded to include emerging technologies and their impacts on privacy and security.

Second, the public and private sector will need more dialogue on future surveillance technologies. Michelle Cayford, Wolter Pieters, and P.H.A.J.M. van Gelder found that when it comes to surveillance technology, the public wants both security and privacy with no tradeoffs.[32] For this reason, states need to engage with their citizens to take the discussion beyond the balance between security and civil liberty. Specifically, Cayford

and Pieters concluded, "Rather than just speaking of providing 'security,' the debate should be sharpened to discuss the effectiveness of the surveillance technology in achieving the security goal."[33] Additionally, states need to articulate that surveillance-technology effectiveness cannot be measured by using traditional crime or security statistics. To illustrate, the public expects to see an inverse correlation between surveillance technology use and crime or security threats, so when the expected pattern is not seen, the public concludes the surveillance technology is ineffective.[34] In reality, states measure surveillance-technology effectiveness by looking at the overall value in achieving outcomes (e.g., disruptions of threats and intelligence validation).[35] There is a need for states and the public to develop a common language to determine acceptable measures of effectiveness.

Future Challenges

Technology is constantly evolving and providing states with more powerful surveillance capabilities. Advancements in real-time connectivity and data analytics, in particular, elevate the privacy threat from omnipresent surveillance. In this section, two technological drivers of change are examined in understanding the future environment: 5th Generation (5G) and 6th Generation (6G) connectivity and AI analytics advancement.

First, 5G-cellular technology is the catalyst launching the world into the Fourth Industrial Revolution with speeds of up to 100 times faster than current cellular networks. 5G is an enabling technology for the Internet of Things (IoT), which is a network of devices and objects with built-in sensors for connectivity and communication. The IoT needs 5G's speed and low latency to move data to and from a massive number of devices and sensors. Many of the IoT connections involve machine-to-machine (M2M) applications in which communication between devices and sensors occur without human intervention. The convergence of 5G and IoT provides the means to create smart cities, smart manufacturing, and autonomous cars, all of which run M2M applications.

In the future, many aspects of life will be monitored by billions of IoT sensors and devices. By 2023, Cisco expects there will be 3.9 billion Internet users and 29.3 billion connected devices, of which half (14.7 billion devices) are for M2M applications.[36] By 2030, not only will the number of connected devices grow to 500 billion,[37] but connectivity speed is also expected to increase with the deployment of 6G-mobile technology.[38] It is important to realize that this vast network of devices and sensors will

be distributed without centralized control or governance.[39] Furthermore, each IoT sensor and device will generate digital data, which can be collected into massive datasets.

Second, AI will be used to interpret the massive datasets generated from IoT devices and sensors. It is through the AI-generated intelligence that an individual can be tracked by facial recognition, smart payment, and smart phones, or that pattern anomalies can be identified as threats. Eventually, AI systems will be integrated so that they can communicate with each other, without human intervention. For instance, autonomous surveillance systems will use AI-enabled camera systems to decide what qualifies as a threat.[40]

Furthermore, the power from other technologies, such as quantum computing and nanotechnology, will be harnessed to make AI even more powerful. Futurists expect that in the next 10 years artificial general intelligence, which is when machines will think like humans, will be achieved.[41] At that time, the digital world will be highly interconnected with over 500 billion devices and sensors, which means cyber attackers have more ways to compromise the security and privacy of individuals. At some time between 2030 and 2050, futurists predict technological singularity, which is the point when AI in machines exceed human intellect, will be achieved.[42] As AI races toward technological singularity, there will be transnational challenges for which the world will be unprepared: they include combat robots, precision biometric attacks, and new types of information warfare. For this reason, futurists also predict that a global AI arms race will ensue.[43]

AI applications will continue to raise ethical concerns, surpassing the current debate on biases. These concerns will be difficult to resolve because there is a lack of transparency with AI algorithms, which are considered intellectual property.[44] In addition, as AI systems are given more decision-making capability, AI algorithm liability, when a machine makes a decision leading to human harm, comes into question. For example, if an autonomous car is involved in an accident, it is unclear if the owner of the system, programmer, or manufacturer is responsible.

When fully deployed, 6G and AI will change every aspect of modern life. These technologies will greatly improve the quality of life of individuals, as they bring advancements to healthcare, transportation, and manufacturing. At the same time, they also will create tremendous challenges and risks, for which societies are unprepared. Since the speed of technological change cannot be slowed, democratic states must take action now

to build strategies and mechanisms to protect civil society while promoting their strategic competitiveness.

The Way Ahead and Conclusion

Although the challenges posed by AI and AI-enabled surveillance technology to democratic values and norms are huge, they are not insurmountable. Rather than provide an exhaustive list of recommendations, this section will suggest foundational steps to take now, so that states can begin to resolve these new challenges to democratic political culture.

Recommendation #1: National AI Strategy

Democratic states should create a national AI strategy because AI is the enabler for the other surveillance technologies. The Atlantic Council recommended using anticipatory governance in developing a national AI strategy to not only define national objectives but also delineate ethical or societal limitations.[45] According to Eleonore Pauwels, anticipatory governance can be used to understand "plausible scenarios related to AI convergence" to imagine hybrid-security threats.[46] Creating a national AI strategy will be challenging for policymakers: they will need to harmonize the conflicting demands of many stakeholders, given the dual-use nature of the technologies, and to consider the impact of associated-emerging technologies (e.g., quantum computing and nanotechnology). Finally, in order for the strategy to succeed, policymakers will also need an implementation plan, with sufficient resources and supporting institutions.[47]

Recommendation #2: Privacy and Security Task Force

Democratic states should create a "privacy and security task force" comprised of government and private sector representatives to ensure that democratic belief, values, and norms are maintained and protected. The first effort of the task force is to ensure that there is a comprehensive privacy and security law, which could be modeled after the EU GDPR and include the other impacts of emerging technologies. The second undertaking of the task force would be to develop a framework to evaluate the social, economic, and human risks and harms created by surveillance and emerging technologies. This will not be an easy undertaking because emerging technologies cross multiple domains, each with differing im-

pacts. The third effort of the task force is to use the framework to examine risks, gaps, and opportunities, to develop policies, and to recommend regulations and laws. The fourth effort of the task force is to regularly monitor the progress of the government toward achieving task force objectives using annual reports, to update the framework, and to proactively respond with policy or regulatory recommendations.

Recommendation #3: Import Control

Democratic states should penalize private companies selling technologies to governments censoring information or conducting mass surveillance by banning their future business interactions with that state. In essence, this recommendation is the inverse of the EU's 2014 ban on the export of technology to governments conducting human rights abuses from surveillance technologies. For example, if U.S. companies were to sell technology to repressive governments, a state could put these companies on a banned-from-importing list, thereby disallowing these companies access to markets in that particular state. This unconventional strategy could prove to be more effective in curbing the behavior of the private sector than export controls because it has a broader impact on global companies by affecting their profits and market access.

In conclusion, surveillance technologies can conflict with the political culture of democratic states by violating the agreement between governments and their citizens for privacy and civil liberty protections. The good news is that by acting now to resolve the political culture debate, democratic states will be in a better position to deal with emerging technologies, which will pose even more ethical and democratic value challenges. Moreover, although the future will bring an accelerated growth of surveillance-driven technology, democratic states will have the strategies, policies, and laws in place to keep pace and maintain the democratic promise to their citizens.

Notes

1 Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment for International Peace, September 17, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

2 Andrea Kendall-Taylor, Erica Franz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy," *Foreign Affairs* 99, no. 2 (March/April 2020): 103, https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.

3 Torin Monahan, "Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance," in *Surveillance and Democracy*, ed. Kevin D. Haggerty and Minas Samatas (New York: Routledge, 2010), 91-110, http://publicsurveillance.com/papers/Monahan_Surv_Democracy.pdf.

4 Nichole Ozer, "Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs," American Civil Liberties Union, September 22, 2016, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-use-social-media-surveillance-software.

5 U.S. Congress, House, Committee Hearing on Oversight and Reform, *Facial Recognition Technology (Part I): Its Impact on Our Civil Rights and Liberties*, 116th Cong., 1st sess., 2019, https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-20190522-SD012.pdf.

6 "Map: Social Media Monitoring by Police Departments, Cities, and Counties," Brennan Center for Justice, July 10, 2019, https://www.brennancenter.org/our-work/research-reports/map-social-media-monitoring-police-departments-cities-and-counties.

7 Rebecca Heilweil, "The World's Scariest Facial Recognition Company, Explained," *Vox*, May 8, 2020, https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement.

8 "Google, YouTube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App That Helps Law Enforcement," CBS News, February 5, 2020, https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/.

9 HiQ Labs, Inc., v. LinkedIn Corporation, 938 F.3d 985 (9th Cir. 2019), http://cdn.ca9.uscourts.gov/datastore/opinions/2019/09/09/17-16783.pdf.

10 Betsy Swan, "Facial-Recognition Company That Works with Law Enforcement Says Entire Client List Was Stolen," Daily Beast, February 26, 2020, https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen.

11 Ryan Mac, Caroline Haskins, and Logan McDonald, "Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA," Buzzfeed News, February 27, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

12 Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

13 Monte Reel, "Secret Cameras Record Baltimore's Every Move from Above," *Bloomberg Businessweek*, August 23 2016, https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/.

14 Connor Friedersdorf, "The Sneaky Program to Spy on Baltimore from Above," *The Atlantic*, August 26, 2016, https://www.theatlantic.com/politics/ar-

chive/2016/08/the-sneaky-program-to-spy-on-baltimore-from-above/497588/.

15 Arthur Holland Michel, "The Military-Style Surveillance Technology Being Tested in American Cities," *The Atlantic*, August 3, 2019, https://www.theatlantic.com/technology/archive/2019/08/military-style-surveillance-air-often-legal/595063/.

16 Baynard Woods, "Baltimore's Newly Revealed Surveillance Program Raises Legal Questions," *The Guardian*, August 26, 2016, https://www.theguardian.com/us-news/2016/aug/26/baltimore-police-surveillance-legal-questions.

17 Kevin Rector, "Baltimore Officials Pitched on Putting Three Surveillance Planes in the Sky at Once, Covering Most of City," *Baltimore Sun*, September 19, 2019, https://www.baltimoresun.com/news/crime/bs-md-ci-cr-surveillance-pitch-20190919-dkurugpjdretrjzcevzlc7eabu-story.html.

18 United Nations Human Rights Council, Forty-first session, "Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A/HRC/41/35, May 28, 2019, accessed April 1, 2020, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session41/Pages/ListReports.aspx.

19 Feldstein, "The Global Expansion."

20 Arkaitz Gamino Garcia et al., *Mass Surveillance: Part 1—Risks, Opportunities and Mitigation Strategies*, (Brussels: European Union, 2015), https://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf.

21 United Nations Human Rights Commission, "The 2019 Report on the Surveillance Industry," United Nations, accessed April 1, 2020, https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx.

22 Elise Thomas, "New Surveillance Tech Means You'll Never Be Anonymous Again," *Wired*, September 16, 2019, https://www.wired.co.uk/article/surveillance-technology-biometrics.

23 Jay Stanley, "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy," American Civil Liberties Union, June 2019, https://www.aclu.org/report/dawn-robot-surveillance.

24 "About," Partnership on AI, accessed April 12, 2020, https://www.partnershiponai.org/about/.

25 Camino Kavanagh, "New Tech, New Threats, and New Governance Challenges: Opportunity to Craft Smarter Responses?" Carnegie Endowment for International Peace, August 28, 2019, https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736.

26 U.S. National Intelligence Council, *Global Trends: Paradox of Progress* (Washington: National Intelligence Council, 2017), accessed April 1, 2020, https://www.dni.gov/index.php/key-global-trends/how-people-govern.

27 "Recommendation of the Council on Artificial Intelligence," Organisation for Economic Co-operation and Development, May 2019, http://www.oecd.org/going-digital/ai/principles/.

28 "Shaping the Future of Technology Governance: Artificial Intelligence and Machine Learning," World Economic Forum, accessed April 1, 2020, https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-artificial-intelligence-and-machine-learning/.

29 Ben Wolford, "What Is GDPR, the EU's New Data Protection Law?" GDPR.EU, accessed April 1, 2020. https://gdpr.eu/what-is-gdpr/.

30 Eline Chivot and Daniel Castro, "The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy," Center for Data Innovation, May 13, 2019, https://www.datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/.

31 "Guidelines 3/2019 on Processing of Personal Data through Video Devices," European Data Protection Board, July 10, 2019, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf.

32 Michelle Cayford, Wolter Pieters, and P.H.A.J.M. van Gelder, "Wanting It All—Public Perceptions of the Effectiveness, Cost, and Privacy of Surveillance Technology," *Journal of Information, Communication and Ethics in Society* 18, no.1 (2019), https://www.emerald.com/insight/content/doi/10.1108/JICES-11-2018-0087/full/html.

33 Michelle Cayford and Wolter Pieters, "The Effectiveness of Surveillance Technology: What Intelligence Officials Are Saying," *The Information Society* 34, no. 2 (2018), https://www.tandfonline.com/doi/full/10.1080/01972243.2017.1414721.

34 Max Bauer, "Review of Studies on Surveillance Camera Effectiveness," American Civil Liberties Union of Massachusetts, accessed April 1, 2020, https://privacysos.org/camera_studies/.

35 Michelle Cayford, Wolter Pieters, and Constant Hijzen, "Plots, Murders, and Money: Oversight Bodies Evaluating the Effectiveness of Surveillance Technology," *Intelligence and National Security* 33, no. 7 (2018), https://www.tandfonline.com/doi/pdf/10.1080/02684527.2018.1487159.

36 "Cisco Annual Internet Report (2018–2023)," Cisco, 2020, accessed April 2, 2020, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf.

37 Fastco Works, "What Will Happen When 28 Billion Devices Are Connected Online?" Fast Company, July 24, 2019, https://www.fastcompany.com/90380201/what-will-happen-when-28-billion-devices-are-connected-online.

38 "5G Evolution and 6G," NTT Docomo, Inc., 2020, https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_20200124.pdf.

39 "Strategic Foresight Analysis," NATO, 2017, accessed April 2, 2020, https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf.

40 Zach Doffman, "Smarter Cities: Will Autonomous AI Surveillance and IoT Now Automate Law Enforcement?" *Forbes*, December 15, 2018, https://www.forbes.com/sites/zakdoffman/2018/12/15/smarter-cities-will-autonomous-ai-surveillance-and-iot-now-automate-law-enforcement/.

41 Christianna Reedy, "Kurzweil Claims That the Singularity Will Happen by 2045," Futurism, October 5, 2017, https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045.

42 Dom Galeon, "Separating Science Fact from Science Hype: How Far Off Is the Singularity?" Futurism, January 30, 2018, https://futurism.com/separating-science-fact-science-hype-how-far-off-singularity.

43 "Autonomous Weapons: An Open Letter from AI and Robotics Researchers," Future of Life Institute, accessed April 1, 2020, https://futureoflife.org/open-letter-autonomous-weapons/.

44 Jonathan Shaw, "Artificial Intelligence and Ethics," *Harvard Magazine*, January-February 2019, https://harvardmagazine.com/2019/01/artificial-intelligence-limitations.

45 Peter Engelke, "AI, Society, and Governance: An Introduction," Atlantic Council, March 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/03/FINAL-AI-POLICY-PRIMER-0220.pdf.

46 Eleonore Pauwels, "The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI," United Nations University, May 2, 2019, https://cpr.unu.edu/the-new-geopolitics-of-converging-risks-the-un-and-prevention-in-the-era-of-ai.html.

47 Engelke, "AI."