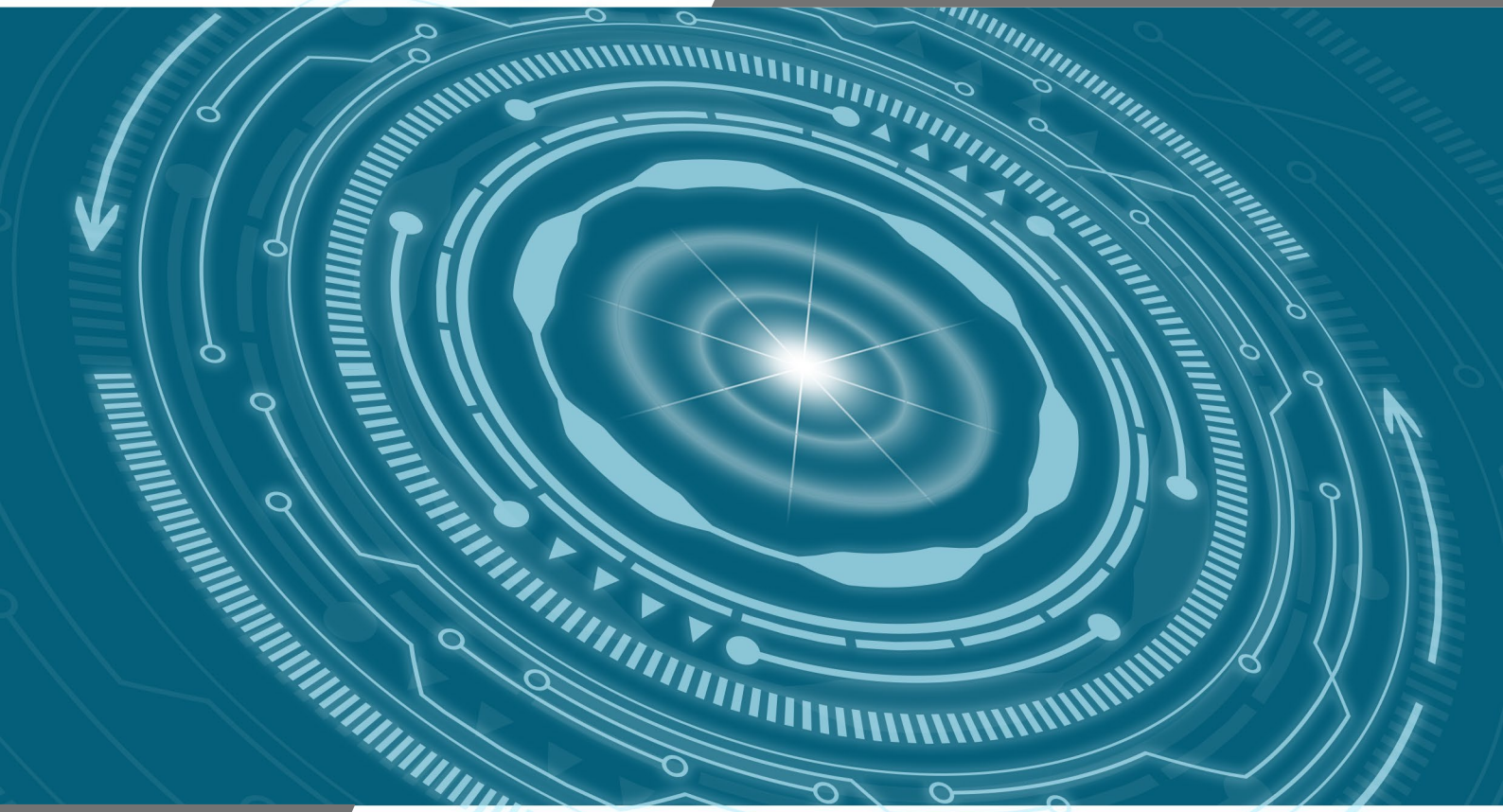
Centre for Economics and Foreign Policy Studies

edam

Cyber Governance and Digital Democracy 2018/2



April 2018

Politics of Digital Surveillance, National Security and Privacy

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has University

Politics of Digital Surveillance, National Security and Privacy

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has University

Executive Summary:

Digital surveillance is a growing global concern, following the Snowden revelations, subsequent national security leaks and the most recent controversy regarding Cambridge Analytica and the Trump campaign. This report explores some of the dilemmas and deadlocks regarding digital surveillance, its extent in democracies and autocracies and how it interacts with the 'surveillance-industrial complex', SIC. SIC is an often-overlooked aspect in the surveillance-privacy debate as it is not necessarily intentions that render surveillance problematic, but its business model. In all political systems there is a secrecy, transparency and surveillance cost which drives a country's willingness to hoard secrets (citizen data, international data transfers) or to disclose some key political information to the public for the sake of legitimacy. A key component of the surveillance-privacy debate in digital space is the technology race, which drives states' unwillingness to disclose policy information due to the increasing costs of acquiring key intelligence in a networked society. Ever-increasing methods and technologies of surveillance and circumvention alike is one of the central reasons on why efforts to regulate and safeguards surveillance mechanisms fail: they simply cannot keep up with the technologically proficient intelligence agencies, nor the ever-resourceful citizen-driven circumvention tools. Good examples in some European countries have focused mainly on making surveillance oversight transparent, while establishing hybrid safeguard mechanisms that are established by proficient technical experts, in addition to bureaucrats or MPs. The failure of surveillance transparency moves largely stem from this technological backwardness of safeguard and oversight mechanisms, as a result of which the public devises its own mechanisms to circumvent, mask or monitor how states manage and process digital intelligence and citizen data. However, especially with the growing threat of terrorism, far-right radicalization and extremist groups emerging in western societies, surveillance is viewed not only politically necessary, but also electorally popular. To that end, public opinion is not unitary and it is itself divided between pro-surveillance and pro-privacy groups. Ultimately, democracies have to come up with the surveillance-privacy balance that conforms to the country's political culture, but also to the universal human rights. The task of oversight in this context is heavy: it has to continuously chase the executive and intelligence community in detecting abuse and excess, while remaining technologically proficient at the same time.

The research has been made possible by funding obtained from the US based Chrest Foundation

Introduction

In mid-March 2018, the data consulting firm Cambridge Analytica was exposed in its extra-judicial dealings with the Trump campaign, where the company harvested more than 50 million Facebook profiles without consent and legal justification. These profiles would later be catalogued into psychological profiles, allowing Analytica to build an algorithm that skewed news results in Facebook users' news feed. According to critics, the move was not just illegal, but it also affected the result of the US election significantly. Cambridge Analytica CEO Alexander Nix was directly involved with Steve Bannon, who was then a major leader within the Trump campaign and would later become the Vice President of the United States; albeit for a short while. Facebook was directly involved as an active actor in the scandal, by willingly exposing 50 million profile raw data to Aleksandr Kogan, a senior Analytica data scientist. Kogan had built 'thisismydigitallife' – a quiz app on Facebook – which profiled an initial 270,000 Facebook users who took the quiz, without the knowledge of this data to be used in a political campaign.[1] Through network analysis methods (friends, interests, likes) Kogan was able to access 50 million users' data through this initial 270,000. The scandal has demonstrated the immense power relations within the politics – surveillance – technology industry nexus, sending a warning sign across the digital world in terms of the safety of personal data, data sharing, data protection and data localization.

As a contested term, digital surveillance can broadly be defined as the act of real-time and retrospective viewing, processing and cataloging of online footprint against the will and/or knowledge of the actor(s) to whom such data belong.[2] At the heart of the debate is consent and knowledge on the part of the actor(s) whose data are being surveilled, and the security, information and intelligence benefits derived from such monitoring. Privacy on the other hand, has a more straightforward definition: freedom from unauthorized intrusion.[3] Although these concepts and the debates surrounding them are not new, the advent of digital interconnectedness, social media and the significant increase in other channels through which digital actors can disseminate and expose personal information, have significantly changed the scale of the debate. Rapidly changing connection technologies create a system where digitized personal information and official data now have multiple points of interception, cannot reliably be deleted, don't expire and can be disseminated across digital platforms at an infinite rate and dizzying speed.

Current debate on the ethics and philosophy of surveillance derive a lot from Jeremy Bentham's 'panopticon'[4] and Michel Foucault's 'panopticism'.[5] The panopticon was an idealized, cost-efficient late-18th century architectural model of a prison, which consisted of a single, central, concealed watchtower that can view all inmates, without inmates being able to see whether they were being monitored or not. Since the prime guardian is concealed and it is impossible for the inmates to predict when they are being monitored - or being monitored at all - the system is based on a collective psychology of fear and being constantly monitored. The concept of panopticon had significant influence over Michel Foucault's works on authoritarianism and surveillance, where he uses the term 'panopticism' to define modern 'disciplinary societies' where the ability to pry and intrude into individuals' lives without being seen and monitored, creates a power mechanism and a culture of control. Instead of elaborate locks, bars or guardians, the disciplinary power of the panopticon architecture works through the threat of invisible surveillance (instead of explicit, visible surveillance). Similar critical interpretations of panopticon also existed in the works of Gertrude Himmelfarb[6] and Jacques-Alain Miller,[7] who defined panopticon as a tool of oppression and social control, which reinforces uniform collective behavior and increases the social costs of deviating from strict cultural modes of behavior. From this perspective, panopticon and panopticism may be viewed as authoritarian modes of state control and social organization, but Foucault's criticism

1 Alvin Chang, "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram," Vox, March 23, 2018, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

2 Marx Gary T., "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance," Journal of Social Issues 59, no. 2 (April 29, 2003): 369–90, https://doi.org/10.1111/1540-4560.00069; Andrew Chadwick and Philip N. Howard, Routledge Handbook of Internet Politics (Taylor & Francis, 2010).

3 Sabrina De Capitani Di Vimercati et al., "Data Privacy: Definitions and Techniques," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 20, no. 6 (December 1, 2012): 793–817, https://doi.org/10.1142/S0218488512400247.

4 Jeremy Bentham, Panopticon: The Inspection House (CreateSpace Independent Publishing Platform, 2017).

5 Michel Foucault, Discipline & Punish: The Birth of the Prison, trans. Alan Sheridan (New York: Vintage Books, 1995).

6 Gertrude Himmelfarb, The Roads to Modernity: The British, French, and American Enlightenments, Reprint edition (New York New York: Vintage, 2005).

7 Jacques-Alain Miller and Richard Miller, "Jeremy Bentham's Panoptic Device," October 41 (1987): 3–29, https://doi.org/10.2307/778327.

went beyond the intrusive qualities of authoritarian states. He was equally critical of social bandwagoning tendencies in democratic countries and a commune's tendency to turn against each other and reinforce the intrusive qualities of panopticon, taking a life of its own regardless of how intrusive a government really is.

Indeed, some argue that the states have been the main beneficiaries of new surveillance methods and tools. Bouncing back from the initial shock of (and lessons from) 2010-2013 Arab Spring and Occupy movements, most states have adapted to the age of social media-driven protests and digital mobilization methods. China's 'Great Firewall' - an umbrella term for a range of filtering and monitoring mechanisms - for example, can use Deep Packet Inspection (DPI) to monitor user entries and keywords, use artificial intelligence to detect social movements and mobilization patterns. China has also recently unveiled police glasses that conduct real-time facial recognition analysis of citizens for law enforcement purposes. Russia has SORM (System for Operative Investigative Activities) laws that allow full surveillance of analog and electronic communications without warrant. United States and European Union states conduct varying degrees of network monitoring, bulk data analysis, collection, and real-time cataloging for intelligence and security purposes.

Democracies and authoritarian states alike engage in wide-ranging mass surveillance practices and often use comparable tools, albeit with varying levels of legal and legislative safeguards. When combined with vast state resources and capabilities, technology has led to the emergence of global 'electronic police states' that have access to historically unprecedented volumes and granularity of citizen information, from their health data to consumption behavior, voter behavior and most states can collect and process cell phone metadata or outright use cell phone tracking to follow individuals in real-time. Even when conducted for national security and counter-terrorism purposes, the scale and detail of mass citizen data collected, leads to rightfully pessimistic observations about individual freedoms and privacy. In the words of Philip Howard, Director of Research at the Oxford Internet Institute: 'we as citizens, have lost the first war of privacy'.[8]

However, citizens aren't the only ones having lost the privacy war. The proliferation of consumer drones and mass availability of high-detail consumer satellite imagery allows citizens to locate and monitor military bases and installations in far-off locations. Social media conflict monitors can collect and curate information, imagery and video from bystanders in a conflict zone and report it with geo-location, date and time, bypassing state propaganda and information channels. Proliferation of open-source analytics initiatives like Bellingcat can use publicly available data sources to conduct 'digital forensics', exploring highly sensitive military topics such as the Russian downing of the MH-17 flight, presence of Russian troops in Crimea, long before such presence was exposed through official channels.[9] In addition, they were the first ones to document and provide evidence of sarin gas attacks in Syria. Most recently, Strava - a mobile app and social networking site for runners - made its user data available for public viewing and search, including route, elevation, speed, timing and geo-location of the logged run. Soon, many users began identifying secret U.S. and other military bases in undisclosed locations in the world, through searchable heat map data, exposing and endangering several such military installations and forward deployment positions around the world.[10]

From this perspective, it is not only citizens that have lost the 'first war of privacy'; states and citizens alike are the losers of this first war. The collectors and hoarders of such data - technology companies, purveyors of surveillance technologies, or Internet Service Providers - haven't really 'won' in the true sense of the word as well. The exposure of new types of collecting and disseminating state secrets and private data alike has led to increased legislative, legal and democratic oversight pressures on these companies, rendering them political players in some of the world's most tense diplomatic and social crises. What really prevailed at the end of the 'first privacy war' has been Foucault's problematization of 'panopticism': the surveillance culture itself and the fear and resentment of being constantly monitored. In this zeitgeist of digital fear and mutual resentment, states, citizens and corporations alike are vulnerable to different aspects of surveillance. This generates a Gordian knot of digital governance, which has global, regional and national implications of political, economic and social nature, forcing all sides to limit their freedom of expression, and self-censor.

8 The Prezi version of this inaugural lecture 'Is Social Media Killing Democracy' can be accessed at: https://prezi.com/cxuukuoovaoc/is-social-media-killing-democracy/

9 MH17 – The Open Source Investigation, Three Years Later: https://www.bellingcat.com/news/uk-and-europe/2017/07/17/mh17-open-source-investigation-three-years-later/

10 Alex Hern, "Strava Suggests Military Users 'Opt Out' of Heatmap as Row Deepens," the Guardian, January 29, 2018, http://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban.

Surveillance-National Security Nexus

Free flow of information is long regarded as the hallmark of democracies. The reason why citizens of Germany and Pakistan have unequal access to their government information or policy processes is a primary driver of why these two countries have different regime types. Yet, this doesn't mean that public access to policy information is uniform across democracies; the contrast is even more marked since the digital communication revolution. Modern democracies have different and often competing interpretations of 'legitimate secrecy', necessary to safeguard a variety of critical national security operations and interests abroad. Political scientist Michael Colaresi argues that all uses and abuses of secrecy requires a 'secrecy cost', which states have to spend in order to be able to render a certain volume of information secret.[11] Such costs are encryption, physical infrastructure to store secrets and elaborate set of power relations that keep these sets of information from public eye (law enforcement, intelligence apparatus etc.), as well as from the enemy's hands. These costs are generally laid out in relation to their strategic utility: either to anticipate enemy actions, deceive adversaries and suppress rival capabilities during crises episodes. The more a state spends on secrecy – infrastructure, cryptography, institutional-organizational capacity or human quality-wise – the better that state is able to distract, mislead and gain strategic upper hand against rival states.

The only type of regime where secrecy costs clash with audience costs on the other hand, are democracies. It is only in democracies that for any one unit of cost spent on secrecy, there is another counter-force from the public, which calls for the transparency of the type of information the state tries to keep secret. Who will oversee the process by which leaders are discouraged to abuse secrecy power? How will the civil society and the parliament exercise its essential duty to hold the decision-makers accountable in their policy choices? Like secrecy is used to mislead and suppress the enemy, it can easily be used to do the same with the public, or oversight institutions. According to political scientist Michael Desch, the difference between how democracies and authoritarian countries deal with secrecy and surveillance is quite similar, although in democracies, it is the public audience costs and policy punishment that creates the biggest difference. In a democracy, the constraints on how leaders process secrecy and surveillance are institutionalized through an elaborate set of interconnected layers that both insulate secrets from public (and adversarial eye), while simultaneously enable the public to pressure the government when there are doubts about the handling of such information. From this perspective, there is also a 'transparency cost' in democracies that such states have to pay to make certain secrets available for public knowledge. Transparency costs interact with secrecy costs, in the sense that every single secret the government makes public for democratic purposes, is also automatically shared with the enemy. To offset the transparency cost of such moves, the state then has to invest even further to make new information secret, or it will lose key comparative advantage against rival states.

However, not all secrets are national security secrets and states often hide essential governance data from the public that has no relation to missile launch codes, or location of offshore airbases. Often, democracies and authoritarians alike, treat governance, financial and social data as 'national security secrets' to hide mismanagement, corruption or poor prioritization. Some of this secrecy may often take the form of using state-owned secrecy and surveillance apparatus to spy on opposition groups, political parties or citizens despite a clear absence of a national security threat. Such public deception markedly increases during conflicts and wars, where the incumbent party or leader uses war-time national security apparatus to secure re-election by misleading public or suppressing political dissent. Western countries that are deployed in civil wars abroad also tend to censor troop casualty figures from the public and the media.

Examples from Canada and Norway – typical top democracies – reveal how the secrecy abuse plagues all regime types. In the 1970s, Canadian Security Intelligence Review Committee (SIRC) reported on a wide-reaching surveillance abuses – 'break-ins, arson and theft targeted at left-leaning press and political parties', including 'a subsequent cover-up' where the Canadian intelligence lied to a ministerial inquiry commission about the extent

[11] Michael P. Colaresi;, Democracy Declassified: The Secrecy Dilemma in National Security by Michael P. Colaresi (Oxford University Press, 2014).

of this program.[12] Through the enforcement mechanism of the Canadian Mounted Police, domestic opposition groups and parties were systematically attacked and disrupted under the guise of national security. In Norway, the abuses that took place during the 1970s could only be exposed in the Lund Commission report in 1990s.[13] These abuses included Norwegian police, intelligence and National Security Authority to conduct a joint effort to spy and disrupt opposition groups that had posed little – if any – national security threat, overt, or explicit.

The dilemma for leaders and decision-making groups processing intelligence and secret information stems from public consent. For any policy to succeed, there has to be public consent and the resultant mobilization for their execution. Similarly, democratic decision-making systems eliminate any miscalculation or misperception, enabling the early discovery of potentially costly mistakes. Authoritarian repression allows leader to both extract the resources from public in the form of over-taxation and corruption, and also to enact policies without their consent. The downside is that the resources generated through forceful methods are usually inferior to the resources generated by democracies, owing the production capacity and speed of more liberal systems. Although technically democratic leaders can mislead domestic public opinion by reframing facts or withholding certain types of information, once such tactics are revealed, they exert disproportionate costs upon those involved in the process, including legal action.

Digital Surveillance – Types and Tools

The tools of digital surveillance and circumvention expand and change along the advances in digital technologies; the faster technology advances, the easier it becomes both to conduct surveillance and deploy circumvention tools against it. To that end, technology itself is neutral and supports all sides of the spectrum in comparable measure, although the side with the highest level of material, technical, human quality and manpower capabilities combined inevitably has the control over the outcomes of technological advances. Digital surveillance can roughly be divided across the domains of data security, imagery, ICTs, geolocation and biometrics. Since the majority of these tools come from traditional signals intelligence practices, their main purpose is to intercept external and domestic communication, data transfers and network monitoring.

Bulk Data Interception. As the founding block of digital communication, data interception sits at the intersection of computer and network surveillance, and concerns both physical data storage units like hard drives, USB flash drives, and Internet-based data transfer, localization and cloud storage applications. This type of surveillance is usually implied within the broader term of digital surveillance. Bulk data interception works through 'packets', the founding block of all digitally-connected communication and transaction. Packets contain content and metadata - which is information regarding the date/time, sender/recipient and location of the transfer. Regardless of distance, packets go through several Internet Exchange Points (IXPs), allowing them to be intercepted, collected and stored by third party agencies or organizations. Tapping undersea fiber-optic cables, for example, is a well-known case, although the majority of bulk data interception takes place through governmental pressures on Internet Service Providers (ISPs).

ICT Monitoring. Internet Communication Technology (ICT) surveillance focuses on human activity on both social media platforms such as Twitter, Facebook or Instagram, but also peer-to-peer communication tools such as Whatsapp, Telegram, Signal or simple SMS tools. ICT surveillance concerns both content (i.e. text of the message concerned), metadata (date, time, location of the message) and network (follow/friends, retweet, 'like' patterns) of a single individual or a group. It is not just the governments of intelligence agencies that monitor ICTs; employers, schools and public wi-fi providers (such as in libraries, restaurants, hotels) also conduct ICT monitoring. Mobile telecommunications interception equipment (IMSI Catchers) that track, identify and record ICTs, intrusive software (malware), network surveillance, data retention

[12] Justin Ling, "The Story of How Canadian Police Committed Arson to Stop a Black Panther Meeting," VICE News, June 2017, https://news.vice.com/en_ca/article/eva8da/story-of-how-canadian-police-committed-arson-to-stop-a-black-panther-meeting.

[13] Dr Hans Born and Ms Marina Caparini, Democratic Control of Intelligence Services: Containing Rogue Elephants (Ashgate Publishing, Ltd., 2013), 145.

systems and deep-packet inspection (DPI) methods are some of the most popular types of ICT content monitoring.

Geo-location and Remote Sensing. Although also embedded within other types of surveillance, location surveillance has its own distinct characteristics. Revolving around mobile device signals and global positioning system (GPS) data, this type of surveillance can be used to infer trajectory, waypoint and coordinates of an individual, group or a building/installation. Most metropolitan cities of the world, including London, Brussels, Paris and New York are embedded with a large network of CCTV cameras that aid in policing, surveillance and behavioral modelling. However, location surveillance has evolved significantly since the advent of CCTVS. LIDAR (Light Detection and Ranging - a laser-based aerial imagery tool), satellite or high-flying aircraft imagery data, and geographic information system (GIS - umbrella name for tools designed to detect, extract and store geographic data) fall into this category.

Biometrics. Biometric markers are the most unique types of personal information, since they are specific to every individual. Fingerprinting for example, is perhaps the oldest and most commonly-used type of biometric data. However, technological advances has enabled surveillance companies to harvest and track newer forms of biometric data as well. Some of the newer biometric identifiers are facial/retinal recognition, voice recognition, skin reflection and thermograms. Various types of biometric surveillance are becoming increasingly common areas with large human influx, such as shopping malls, stadiums, banks, airports and transportation. The granularity of biometric data, as well as the ease with which they can be stored and used for long periods of time, have led to their rise in popularity, especially with high population density areas. For example, China has recently began collecting biometric data of all Xinjiang residents through a program titled 'Physicals for All', building a database of iris scans and blood types of around 11 million Xinjiang residents.

Internet of Things. IOTs are comprised of consumer-facing devices that are structured on automated communications between machines. Most household devices are IOT-enabled nowadays, which renders common items like dishwashers, TVs, home assistants and fridges. Users can turn their curtains on and off, adjust water temperature, cooking and home heating controls from a remote location, using dedicated apps. Most modern home safety and alarm systems are also IoT-enabled, with sets of CCTV cameras installed within the house. Users can monitor such camera feeds and monitor homes through Internet-enabled applications. Data collected and stored in IoTs concern behavioral patterns such as time of arrival and time spent in a home or workplace, speech-movement detection, purchasing and consumption patterns of individuals or organizations. Without safeguards, IoT surveillance can provide large-scale private citizen data on time spent outside homes and workplaces, types of online purchases made and social network (family and close friend information), enabling mass governmental intrusion into citizens' everyday lives. The threat is beyond states, however, as hackers too can exploit IoT homes to spy on individuals, or cause these units to malfunction, leading to serious bodily harm.

A major by-product of the booming of the surveillance industry in the last decades is the emergence of the 'Surveillance-Industrial Complex'.[14] The 'Surveillance-Industrial Complex' (SIC) derives from the well-known post-World War 2 concept of the military-industrial complex (MIC), which denotes a symbiotic relationship between a nation's armed forces and its private arms production companies. The argument in favor of such relationship was increased military production and the sustenance of a vast weapons industry that is responsive to the immediate and ever-changing needs of the nation's military. The best-known argument against it however, was articulated by the U.S. President Dwight D. Eisenhower, who asserted that arms industry corporations would have a disproportionate influence on foreign and defense policy, creating the material conditions for permanent reliance on peak military production, as well as immense influence on national security threat perception.[15] The combination of the military's reliance on large weapons industry companies, these companies influence over the Congress and the Congressional influence on military policy formed one of many 'iron triangles' US politics. Such iron triangles would then impair the democratic functioning of the system through the influx of vast amount of lobbying funds that

[14] Kirstie Ball and Laureen Snider, The Surveillance-Industrial Complex: A Political Economy of Surveillance (New York: Routledge, 2013); David Lyon, Kirstie Ball, and Kevin D. Haggerty, Routledge Handbook of Surveillance Studies (New York: Routledge, 2012).

[15] Eisenhower, Dwight D. "Farewell address." Washington, DC 17 (1961).

would advocate in favor of US involvement in more conflicts, rendering the country more war-prone.

SIC follows a similar logic, although the relationship between technology companies and the governments isn't mutually beneficial as in MIC. It is also not confined to U.S. politics. Rather, SIC refers to nations' security and intelligence agencies entering into a one-sided extractive relationship with private sector technology and surveillance companies. By creating a public-private surveillance nexus, governments and intelligence agencies harness - often extra-judicially - large volumes of citizen data processed by private companies and hold the enforcement powers to bend these companies to their will. State agencies' access to private-sector databases create both legal and democratic problems, since most states have already collected large troves of private citizen data before the promulgation of laws that limit the extent of such surveillance practices. Even when such laws are in place, the speed with which surveillance technologies evolve, renders recent laws quickly obsolete, allowing agencies to circumvent laws and legislation to use newer forms of digital surveillance.

Governments gain three major benefits from SIC. First, it generates a 'swarm intelligence network' in which large volumes of unstructured personal data are collected into a central nexus that allows detailed profiling. Second, the political and financial costs of surveillance are transferred from governments to tech companies. Normally, agencies will have to invest in physical infrastructure (supercomputers) along with highly-trained human capital (data scientists, engineers) in order to conduct mass digital surveillance. Through SIC, governments are able to freeride significant amount of the base costs spent by tech companies. Third, if the surveillance program is exposed, most of the audience costs (criticism and public shaming) are met by the companies, rather than the state, for allowing agencies to harvest and exploit personal data that users entrust. In today's technology environment, SIC allows for an unprecedented size and granularity of private data, rendering governments as the hubs of vast networks of personal information. On the other hand, however, the SIC creates a security dilemma over the long-term by rendering states more defensive and making them more forceful in requiring data and systems localization. While the free flow of data and information is regarded as essential to trade, finance and global interconnectedness, the intrusion of the world's intelligence agencies into the chokepoints of data transfers (cloud systems, underwater fiber optic cables) has generated increasing demands for localization. By localizing systems and data, countries seek to emphasize 'data nationalism' by preventing snooping by foreign agencies or secure their national data in case of mass data harvesting. Localization however, renders such data increasingly vulnerable to cyber-attacks and increase the costs of data protection by requiring the construction of physical storage systems from scratch, recruiting highly trained human assets and building storage protection networks. While data localization is an internationally undesired move, that slows trade, transfers and finance, increasingly more nations find this necessary given the exposure of key citizen data to foreign intelligence agencies.

Current Trends in Digital Surveillance

Surveillance-privacy battle has been a by-product of our wider problems with adapting to technological advances. That's why threats to privacy and remedies of protection have usually followed each other in a tight chronological order. 'The right to be left alone' for example, appears first in 1890s. In the same decade, fingerprinting was introduced to identify people and establish well-maintained physical datasets of personal identification. In the US, a 1928 court order has ruled in favor of seizing electronic communications in times of 'threats to national security', although what national security constituted was left unaddressed. The Project MINARET and SHAMROCK, were to US Government exercises that spanned across 1967-78, that intercepted and collected all electronic communications of US citizens in a coordinated FBI-CIA, BNDD and DoD effort to serve as domestic counter-espionage against the USSR.[16] In 1967, 'Katz-vs-US' court battle led to a legal precedent that ruled enforcement agencies to get a warrant before intercepting personal communications.[17] With the digitization of fingerprinting and establishment of large personal datasets of citizenship information, digital identity theft becomes common, leading

[17] Katz v. United States, 389 U.S. 347 (1967): https://supreme.justia.com/cases/federal/us/389/347/case.html

[18] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," IEEE Security Privacy 9, no. 3 (May 2011): 49–51, https://doi.org/10.1109/MSP.2011.67.

to the boom in anti-intrusion and anti-virus software industry. Following the advent of HTTPS in 1995, spyware and bugs become commonplace, leading to anti-virus and anti-malware companies becoming increasingly relevant from a political standpoint into the 2000s. This was especially after the exposure of Stuxnet - a computer virus that hinted at the possibility of large-scale physical destruction - and the invention of new forms of air-gapping and protection mechanisms.[18] Following Snowden revelations and the exposure of the extent of NSA surveillance behemoth, EU introduced the 'Right to be Forgotten', along with the proliferation of public-level crowdsourced initiatives of privacy and anonymity networks.[19]

Although the history of surveillance is quite old, a meaningful tracing of modern digital and interconnected surveillance debates could go back to post-September 11 security setting. It is mostly post-9/11 US surveillance practices from which much of our modern debates on digital surveillance (like bulk metadata collection, biomedical surveillance and network interception) sprung from. Much of these George W. Bush-era US programs and legal-legislative moves to bring them under legitimacy have influenced European countries, and set important examples and state-behavioral standards for the rest of the world. In the United States, the National Security Agency (NSA) started to collect and store US citizens' phone calls, emails and other digital activities without a warrant following legal easing of surveillance safeguards after the USA Patriot Act of 2001. Such practices (under a Bush-era program titled 'Stellarwind'[20]) were conducted largely without public knowledge, and it was only in 2008 that the program entered the Congressional radar. In 2008, the Congress brought the program under the jurisdiction of the Foreign Intelligence Surveillance (FISA) Act, which outlined legal US procedures for the processing of physical and electronic surveillance data related to external state actors and individuals suspected of espionage and terrorism. Since then, the controversial Section 702 of the act ("allows the government to obtain the communications of foreigners outside the United States, including foreign terrorist threats."[21]) came under increased controversy and political debate. The law legalized US agencies' access to Silicon Valley firms, in addition to broadening existing access to telecommunication companies, for the purposes of broadly defined 'foreign intelligence operations'.[22] Despite widespread Congressional criticism of over-reach and media awareness-building on the matter, the Congress extended the law for 5 years in 2012.

Perhaps the most critical turning point in the surveillance-privacy debate was the 2013 NSA 'Snowden' leaks, detailing the scope, depth and extra-judicial extent of US spying programs.[23] An NSA contractor, working with Booz Allen Hamilton, Edward Snowden downloaded around 1.5 million national intelligence files, leaking it to the press and fleeing from his base in Hawaii to Hong Kong, before getting stuck in Moscow. 'Snowden leaks' contained NSA's mass collection of millions of Verizon phone records, an Obama-era order for the collection of overseas targets for cyber-attacks and an NSA program called 'EvilOlive' that logged US citizens' Internet and email metadata real-time.[24] The leaks also demonstrated how the British GCHQ - Government Communications Headquarters - spied on politicians attending G-20 meetings in London in 2009, and its regular practice of tapping into fiber-optic cables to intercept and catalog email messages, Facebook shares, browser histories and Internet calls, sharing this information with the NSA.[25] Although the exposure of state secrets rendered Snowden a public enemy in the US, in the rest of the world, these disclosures have initiated a significant global momentum for high-level norm-building and legal regulations. Yet, the process has also alarmed NGOs, international companies and individual citizens, who now witnessed how extreme mass surveillance regulations were becoming. This ushered a new period of citizen-led

[19] Jeffrey Rosen, "The Right to Be Forgotten Symposium Issue: The Privacy Paradox: Privacy and Its Conflicting Values," Stanford Law Review Online 64 (2012 2011): 88–92.

[20] David L. Altheide, "The Triumph of Fear: Connecting the Dots about Whistleblowers and Surveillance," International Journal of Cyber Warfare and Terrorism (IJCWT) 4, no. 1 (January 1, 2014): 1–7, https://doi.org/10.4018/ijcwt.2014010101.

[21] FISA Section 702: https://intelligence.house.gov/fisa-702/

[22] Stephanie Cooper Blum, "What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform," Boston University Public Interest Law Journal 18 (2009 2008): 269–314.

[23] S. Landau, "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations," IEEE Security Privacy 11, no. 4 (July 2013): 54–63, https://doi.org/10.1109/MSP.2013.90.

[24] Glenn Greenwald and Spencer Ackerman, "How the NSA Is Still Harvesting Your Online Data," the Guardian, June 27, 2013, http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

[25] Source: BBC/Panorama, "Edward Snowden: GCHQ Wants to Own Your Phone – Video," The Guardian, October 5, 2015, sec. US news, http://www.theguardian.com/us-news/video/2015/oct/05/edward-snowden-gchq-wants-own-your-phone-video.

privacy initiatives, emergence of new circumvention tools and significant pressures on legislatures to democratize and legitimize spying activities. It has also led to a new status quo of mutual mistrust and intelligence security dilemma between nations - and even NATO allies - who took measures to bolster their surveillance capabilities both for inter-state competition, as well as for domestic monitoring of foreign digital intelligence activities.

Currently US, Russia and China forces technology companies to create 'backdoors'[26] that will allow intelligence agencies to circumvent encryption and user passwords to access information on devices at will. US tech firms are also under pressure by China to open up their source code for review. From China's point of view, this source code audit is necessary to circumvent possible US 'spy software' integrated into these devices.[27] Washington's narrative on the other hand, is that the US isn't interested in adding backdoors to China-bound technology exports, but mainly worried about how such audit processes could pressure tech companies into installing Chinese spyware into US-made devices.[28] This spyware dilemma is the reason why most technology-exporting countries have created their own version of backdoors or source code audit processes in technology exports and imports. Similarly, both NSA and GCHQ have used submarines to tap into underwater fiber-optic cables to intercept and harvest global internet communications.[29]

It is hard to draw a clear line between US surveillance practices and those of authoritarian regimes, the only difference being the direction of regulations. In most democracies, leaks and non-state discoveries of surveillance practices trigger the need for legal oversight, whereas in authoritarian countries, intelligence requirements determine the extent of oversight, where national security requirements - not oversight necessities - drive the direction of legislation. In Russia for example, System Operational-Investigatory Measures (SORM) has long been the basis of lawful surveillance of digital communications and telecommunication networks.[30] A set of legal and technical requirements that define the legal limits of surveillance, SORM has been updated three times so far, with SORM-1 implemented in 1995 (obligatory installment of Federal Security Service - FSB - hardware to all telecom operators), SORM-2 in 1998 (additional FSB hardware to be installed on Internet Service Providers' servers) and SORM-3 in 2014 (a more detailed wiretapping system for targeted digital surveillance, with separate specifications for IPv4-IPv6 networks, IMSI-IMEI data and POP, SMTP and IMAP4 addresses. Legally, SORM enables surveillance agencies to track and store metadata without a warrant, but warrant is still required for content. Even when agencies have a warrant, they do not have any responsibility to display the warrant to the target ISP or company, but only for intra-agency audit purposes. A 2016 'Yarovaya Law' (named after Irina Yarovaya - a senior member of the ruling United Russia party) eased these restrictions further, ordering all ISP and communication companies to automatically transfer all metadata on agency request, without a warrant.[31]

Chinese surveillance system on the other hand, is mainly driven by Tibet and Xinjiang-Uighur disputes.[32] Chinese surveillance law is similar to Russia's in terms of the direction of legal requirements (i.e. law, driven by security necessities), however China goes one step ahead and encourages 'social supervision', where citizens are required to aid and assist the government agencies in monitoring violations, suspicious digital activity.[33] Some of the recent legal requirements are compulsory real-name register for online video uploads, government-made reporting and complaint apps that allow Chinese citizens to take part in

[26] "Hacker Lexicon: What Is a Backdoor?," WIRED, accessed March 28, 2018, https://www.wired.com/2014/12/hacker-lexicon-backdoor/.

[27] Dave Lee, "China and US Clash over Backdoors," BBC News, March 4, 2015, sec. Technology, http://www.bbc.com/news/technology-31729305.

[28] Ben Goad, "New Pressure on US Tech to Comply with China's Access Demands," Text, TheHill, October 16, 2015, http://thehill.com/policy/cybersecurity/257194-new-pressure-on-us-tech-to-comply-with-chinas-access-demands.

[29] Ewen MacAskill et al., "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications," the Guardian, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[30] Andrei Soldatov and Irina Borogan, "Inside the Red Web: Russia's Back Door onto the Internet – Extract," the Guardian, September 8, 2015, http://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet.

[31] Alec Luhn, "Russia Passes 'Big Brother' Anti-Terror Laws," the Guardian, June 26, 2016, http://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws.

[32] Tom Phillips, "China Testing Facial-Recognition Surveillance System in Xinjiang – Report," the Guardian, January 18, 2018, http://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report.

[33] Anna Mitchell and Larry Diamond, "China's Surveillance State Should Scare Everyone," The Atlantic, February 2, 2018, https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/.

national surveillance, social credit system - which 'ranks' social behavior of citizens, bulk bio-medical data collection and cataloging, real-time facial recognition database and AI-based monitoring of the country's more than 20 million CCTV cameras.[34] As of 28 June 2017, China passed a new National Intelligence Law, which created expansive legal authority for the Ministry of National Security and the Internal Security Bureau of the Ministry of Public Security to collect any and all digital citizen and company data at will, without any warrant.[35] The law specifically shies away from creating a legal oversight mechanism, although a political oversight mechanism is in place, rendering these surveillance activities subject to political monitoring by the 'leadership core' - the Chairman of the Communist Party: Xi Jinping.

Compared to the US, China and Russia, European Union countries are following a slightly different path. 15 years after the signing of the 2000 'Safe Harbor' agreement (2000/520/EC), a data-sharing deal that enabled the legal transfer of EU citizens' personal information and public data to the United States, Court of Justice of the European Union (CJEU) issued a 2015 decision where Snowden-era revelations of extra-judicial mass surveillance made it impossible to ascertain that such data would be sufficiently protected when shared with US partners.[36] This created a significant divide between the US and the EU, where the latter attempted to shield the former from unlawful surveillance instructions into European personal data architecture. Yet, the secrecy-privacy dilemma plays out in individual European countries as well. In November 2017, Britain passed the Investigatory Powers Act (IPA), which allowed GCHQ to conduct mass collection, cataloguing and interception of 'overseas-related' digital activities.[37] This Act provided a legal basis for 'bulk data acquisition' through a warrant, which authorizes the collection of large amounts of transmission, metadata and equipment (hardware data), along with mass-hacking of digital networks throughout the globe. There are three layers of political and legal oversight mechanisms behind bulk collection. Head of intelligence service, or a representative must submit a formal rationale to the Secretary of State. The Home Office then has to conduct an internal proportionality analysis - a report which is sent to the Judicial Commissioner for legal fit. Termed as 'the double-lock mechanism' (both legal and political safeguards against abuse) this safeguard allows for bulk collection for up to 6 months, subject to renewal through the same pipeline.[38] A current problem with the Act is that it doesn't specify what measures foreign individuals could take in the event of an abuse or misjudgment on the part of the agencies in question.

In Germany on the other hand an October 2017 'Communications Intelligence Gathering Act' has authorized the Federal Intelligence Service (BND) for bulk collection overseas, as well as large numbers of Germany based Internet Exchange Points (IXPs), the latter making the country a unique player in worldwide Internet traffic, as well as surveillance activities of other intelligence organizations around the world.[39] Despite the law's seemingly 'domestic' concern, the physical location of IXPs in Germany renders the law truly global, and BND, a major player within the systemic surveillance debate.[40] In this law, BND is given an initial authority to perform a 'test of relevance' - which use big data and machine learning text-as-data practices to catch terms and word exchanges that might constitute a national security problem. These tests are run by the BND without any legal or political oversight, the only authority being the Director of the Agency. These words must be deleted after two to four weeks depending on the purpose of the collection. A German Constitutional Court had issued an earlier verdict in June 2013 that the BND must not disclose these search and surveillance terms to the German Parliament's Special Parliamentary

[34] Rachel Botsman, "Big Data Meets Big Brother as China Moves to Rate Its Citizens," WIRED UK, October 2017, http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion.

[35] "China Passes Tough New Intelligence Law," Reuters, June 28, 2017, https://www.reuters.com/article/us-china-security-lawmaking/china-passes-tough-new-intelligence-law-idUSKBN19I1FW.

[36] Samuel Gibbs, "What Is 'Safe Harbour' and Why Did the EUCJ Just Declare It Invalid?," the Guardian, October 6, 2015, http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection.

[37] Scott Carey, "Investigatory Powers Act: What You Need to Know," ComputerworldUK, January 2018, https://www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/.

[38] Privacy International, "A New Era of Mass Surveillance Is Emerging Across Europe," Medium (blog), January 17, 2017, https://medium.com/privacy-international/a-new-era-of-mass-surveillance-is-emerging-across-europe-3d56ea35c48d.

[39] Jenny Gesley, "Foreign Intelligence Gathering Laws: Germany," Web page, June 2016, https://www.loc.gov/law/help/intelligence-activities/germany.php.

[40] Andre Meister, "How the German Foreign Intelligence Agency BND tapped the Internet Exchange Point DE-CIX in Frankfurt, since 2009," netzpolitik.org (blog), March 31, 2015, https://netzpolitik.org/2015/how-the-german-foreign-intelligence-agency-bnd-tapped-the-internet-exchange-point-de-cix-in-frankfurt-since-2009/.

Fact-Finding Commission established right after Snowden leaks, due to 'extreme significance of the list' compared to public interest.[41] Similar to the UK, head of BND has to formally apply to the Federal Chancellery with a formal report detailing the duration and the scope of the bulk collection required, with a maximum request duration of 9 months. A 3-member evaluation committee, made up of two independent judges and a federal public prosecutor, has to make a decision from a legal point of view. The panel is also the primary authority that issues a verdict to renew the 9-month duration, as well as to cancel the collection process in the event of abuses.

France passed the International Electronic Communications Law following the November 2015 attacks in Paris, enabling Directorate General for External Security (DGSE) to tap, catalog and store digital data from and to foreign countries, similar to the powers given to GCHQ and BND.[42] Unlike UK and Germany, in French case it is not the head of DGSE that directly requests bulk collection, but has to go to the Minister of Defense, Interior or Finance, who can issue a request to the Prime Minister's Office. Once issued, the storage period of communication content is up to one year, and communication metadata, up to 6 years.[43] With additional requests, encrypted content and metadata can be stored for up to 8 years. The National Commission for the Control of Security Interceptions (CNCIS), made up of 9 members (2 judges, 2 State Council members, 4 MPs, one electronic communications expert) are informed for legal fit after the Prime Ministerial decision - not before, as the law doesn't require consultation to any independent authority before the bulk collection decision. CNCIS can only launch investigations and inquiries after the decision, and only after the formal complaint of an individual or organization.

Although relatively more concerned about privacy, safeguards and legal oversight compared to the US, Russia and China, European laws too are explicitly vague in terms of proper oversight mechanisms and safeguards against abuse. Even in the tightest case of the UK, there are limits to how much review Judicial Commissioners can undertake, as well as a significant time pressure between the urgency of the bulk data collection request and the duration of the legal and technical oversight required to approve the request. Furthermore, all three European legal cases leave intelligence sharing on collected bulk data outside the scope of the national laws. Critics point to the fact that much of the surveillance abuse can easily take place in the intelligence sharing mechanism, which concerns external relations, than domestic safeguards that emphasize oversight within internal relations.[44] Across Europe, rising far-right and its electoral popularity has rendered restrictive mass surveillance powers popular. Set by the Orwellian examples of surveillance technology pioneers US, China and Russia, European countries too, are increasingly more concerned about not being left behind in the global surveillance race. In a typical security dilemma scenario, those countries that employ strict oversight and legal anchors to their signals intelligence agencies, are having to respond to ever-increasing speeds at which digital intelligence is produced and processed, in a slower and often late manner. Both European Court of Human Rights and Court of Justice of the European Union legislations are growing increasingly irrelevant in individual European countries, that are having to balance between human rights concerns, intelligence competition and large electoral popularity of surveillance policies.

41 Marcus Lütticke, "New Leaks Show Germany's Collusion with NSA | DW | 21.06.2014," DW.COM, June 2014, http://www.dw.com/en/new-leaks-show-germanys-collusion-with-nsa/a-17726141.

42 Kim Willsher, "France Approves 'Big Brother' Surveillance Powers despite UN Concern," the Guardian, July 24, 2015, http://www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers.

43 Nicolas Boring, "Foreign Intelligence Gathering Laws: France | Law Library of Congress," web page, December 2014, https://www.loc.gov/law/help/foreign-intelligence-gathering/france.php.

44 Cynthia Wong, "Big Brother Is Watching: Why We Should Fear Surveillance in the New World Order," Newsweek, February 7, 2017, http://www.newsweek.com/state-surveillance-europe-populism-cctv-citizens-553857.

Public Pushback: Privacy and Circumvention Tools

The sophistication of circumvention tools owe partly to technological improvements, but largely due to the absence of a strong legal and political social contract between states, tech companies and citizens over the extent and depth of surveillance practices. Such democratic and legal deficit has forced citizens to look after their own defenses when it comes to privacy, generating a significant momentum in favor of elaborate and ever-changing patterns of secrecy and anonymity. In that, intelligence agencies' failure to comply with national and international laws,[45] along with the absence/weakness of national laws or oversight, has forced individuals and activists into a 'self-help' reflex, generating a strong and steady momentum towards establishing reliable circumvention regimes and awareness of personal identity and data protection measures. What separates a circumvention tool from an anonymization tool is that the former is designed to bypass a network or website restriction, whereas the latter aims to protect a user's identity.[46] Often these tools are used interchangeably; for example Tor - a randomized re-routing-based encrypted circumvention system - can be used to protect a user's privacy by anonymizing information, although its primary build purpose is to circumvent filtering and blocking applications.[47]

There are three main types of online identities: 'transactional identity' refers to the set of narrowly-defined information that allows an individual to engage in a specific task or transactional relationship with a company or organization such as banks, government or insurance companies. 'Social identity' is the sum of data posted online by the individual, such as text (i.e. tweets, Facebook posts), image (selfie), location (check-ins) and time (post frequency and timing). Finally, a 'professional identity' refers to the individual's set of skills, competencies and work experience, specifically curated for business and job-related purposes.[48] Most Internet users aren't aware of the interaction between these three identities; namely, how their private digital data can be used by hiring agencies and governments, although 'cross-harvesting' of these seemingly separate types of data is not only easy, it is also how the ICT business model is configured. It is also through the cross-feed between these three types of identities that surveillance mechanisms make inroads into individuals' personal lives and data. For example, most users are unaware of the fact that governments can track their email addresses across multiple platforms (Twitter, Instagram, Amazon, Netflix), even though a user might have a different username or credentials in each of the four. Although some of the easiest and best-known ways of protecting personal information are confined to password security, restricting online share settings and using IP-blocking tools, the current state of modern surveillance can easily bypass them. Privacy-enhancing technologies (PETs) are thus, a separate industry that works by developing new defenses against the advances in surveillance technologies, and work by masking users' web traffic in a way that bypasses or misleads digital barriers that are blocking and filtering a particular content or a set of websites.[49] PETs are divided into two main categories: network-end PETs and user-end PETs. Network-end PETs aim to anonymize and mask user's interaction with the web through:

- web-based proxies that allow access to blocked and censored websites without giving away user information, IP and location (such as kProxy, Whoer.net, Dontfilter or AnonyMouse)
- encrypted proxies that scramble user connection to the server and reinforce the effect of web-based proxies,
- virtual private networks (VPNs) that divert user traffic through another server, misleading some (but not all) surveillance tools, (such as Hotspot Shield, Hamachi, or Privoxy)
- anonymity networks that route web browsing traffic (such as Tor)
- end-to-end encrypted messaging applications (such as

[45] Article 17 of the International Covenant on Civil and Political Rights, UN General Assembly resolution 68/167, UN Human Rights Committee General Comments 27, 29, 31 and 34.

[46] Yi Mou, Kevin Wu, and David Atkin, "Understanding the Use of Circumvention Tools to Bypass Online Censorship," New Media & Society 18, no. 5 (May 1, 2016): 837–56, https://doi.org/10.1177/1461444814548994.

[47] Damon McCoy et al., "Shining Light in Dark Places: Understanding the Tor Network," in Privacy Enhancing Technologies, Lecture Notes in Computer Science (International Symposium on Privacy Enhancing Technologies Symposium, Springer, Berlin, Heidelberg, 2008), 63–76, https://doi.org/10.1007/978-3-540-70630-4_5.

[48] Liam Bullingham and Ana C. Vasconcelos, "'The Presentation of Self in the Online World': Goffman and the Study of Online Identities," Journal of Information Science 39, no. 1 (February 1, 2013): 101–12, https://doi.org/10.1177/0165551512470051.

[49] Yang Wang, "Privacy-Enhancing Technologies," Handbook of Research on Social and Organizational Liabilities in Information Security, 2009, 203–27, https://doi.org/10.4018/978-1-60566-132-2.ch013.

Signal or Telegram)
- reverse proxies that enable authentication, decryption and caching for the purpose of masking user information,
- SSH tunneling, that 'tunnel' user traffic data through a specifically encrypted channel, providing access to blocked content, without disclosing user information (such as PuTTY)

User-end PETs on the other, are software-based applications that start encryption, masking and diversion processes at the user-level. Some examples are CGI proxies that scramble network data before the user accesses the browser, HTTP proxies that establish direct circumvention linkages between them to bypass network-level surveillance and p2p (peer-to-peer) systems that crowdsource all functions of user-end proxies between trusted servers and machines.[50] Although these tools have enabled large percentages of the populations living under surveillance and censorship to circumvent some of these controls, the silencing effects of surveillance is still strong. Although tools that empower free speech and anonymity are becoming more widely available than ever, they aren't always suitable for privacy protection. Most importantly once a government has the full control of the communication infrastructure of a country, it can bypass almost all circumvention and anonymity tools, intercepting an overwhelming majority of interactions in encrypted platforms.

In addition to technical measures, there are ongoing civil society resistance movements against extreme surveillance measures of states. These groups can be divided into six main categories: privacy-centric movements, civil liberties organizations, human rights organizations, consumer protection initiatives, digital rights activists and 'single issue initiatives' that focus either on a particular surveillance technology (i.e. backdoor exploitation), or on a type of information (i.e. personal data), vulnerable people (i.e. Facebook users), or grievances of a particular business sector.[51] In the Philippines for example, a 2012 law introduced granted significantly broadened and unchecked powers for enforcement authorities to track information online. This later spilled-over into extreme censorship behavior, whereby the agencies began to block and censor content that belonged to political opposition groups, instead of criminal organizations.[52] The resultant public protests have resulted in the establishment of FMA (The Foundation for Media Alternatives), a digital rights group that remained a central component of Internet privacy and digital freedoms in the country, through submitting petitions and reports to the parliament on protecting freedom of information.

It was also a joint concerted effort by numerous European digital rights groups that the EU had annulled the Safe Harbor agreement in October 2015. Then in February 2017 a letter by global civil society groups - Access Now, Bits of Freedom, Chaos Computer Club, Civil Liberties Union for Europe, Electronic Frontier Foundation, European Digital Rights, FITuG, Föreningen för Digitala Frioch Rättigheter Initiative für Netzfreiheit, IT-Political Association of Denmark, La Quadrature du Net, OpenMedia, Open Rights Group, Panoptykon Foundation, Son tus datos, Statewatch, and Vrijschrift – that had initiated the process by which the European Union considered suspension of the Privacy Shield data-transfer agreement, the successor to the Safe Harbor Agreement. The rising surveillance arms race between developed countries (including between the US and European countries, as well as within the EU) has resulted in the emergence of a well-knit network of digital rights activists, responding in unison against some of the most problematic state intrusions into global privacy.[53] Given the most problematic set of advanced abuses taking place in the US, it is also home to some of the most rigorous digital rights groups, including American Civil Liberties Union, Stanford's Digital Civil Society Lab and the Digital Impact Lab. In Europe, the European Digital Rights (EDRi) is another significant player, working as an umbrella organization for most major European digital rights initiatives, along with the European Privacy Association. The Sweden-based Pirate Party too, has grown into a global node of digital rights activism with active affiliate parties across the world.

[50] Simone Fischer-Hbner and Stefan Berthold, "Chapter 43 - Privacy-Enhancing Technologies1," in Computer and Information Security Handbook (Second Edition), ed. John R. Vacca (Boston: Morgan Kaufmann, 2013), 755–72, https://doi.org/10.1016/B978-0-12-394397-2.00043-X.

[51] Seeta Peña Gangadharan, "The Downside of Digital Inclusion: Expectations and Experiences of Privacy and Surveillance among Marginal Internet Users," New Media & Society 19, no. 4 (April 1, 2017): 597–615, https://doi.org/10.1177/1461444815614053.

[52] Jessamine Pacis, "State of Surveillance in the Philippines," Foundation for Media Alternatives (blog), April 7, 2016, https://www.fma.ph/2016/04/07/state-of-surveillance-in-the-philippines/.

[53] Colin J. Bennett and Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (New York: Routledge, 2017).

In the United States, the surveillance-privacy debate reached its momentous moment in early 2018, when the Congress debated extending the Section 702 of the FISA Amendments Act that will continue to enable the government to collect citizen data without warrant, through Google and AT&T service providers.[54] The pro-privacy camp, led by a bipartisan group of liberty-oriented legislators aimed to track back some of the most excessive aspects of state surveillance, whereas the Trump-led camp, which included House Republics and the intelligence community sought the continual expansion of surveillance capabilities. Pro-privacy advocates, backed by a strong civil society network, seek to ban the practice whereby FBI and NSA read emails, text messages and mass collects the content of digital messaging without a court order. The intelligence community on the other hand argued that this move would weaken the US, against Russian and Chinese surveillance capabilities that are being expanded radically without any legal or political oversight. Eventually, the Congress passed another law, the CLOUD Act, which allowed US law enforcement agencies to harvest and log any data stored anywhere in the world, without following foreign data privacy rules.[55] In addition, it allowed the US President to negotiate exclusive deals with other nations to allow them to do the same with US-stored data.

Surveillance - Privacy Debate: An Introduction to main positions

Current state of the surveillance-privacy debate concerns domestic and international politics equally, with policy linkages and spill-overs. At the national level, the state-side of the debate favors the use of surveillance as part of a national security strategy and its components such as counterterrorism, counter-narcotics and criminal profiling and so on.[56] Especially with the growing threat of terrorism, far-right radicalization and extremist groups emerging in western societies, surveillance is viewed not only politically necessary, but also electorally popular.[57] Society-side of the debate however, is concerned chiefly with the extent and scope of surveillance (how much surveillance is too much) and which legal and legislative oversight mechanisms are employed to prevent abuse and attain public consent. On the other hand, despite greater legitimacy of UK style 'double-lock' safeguard mechanisms, such models delay intelligence processing and cause agencies to miss critical intelligence, often at the anger of the public. Governments usually believe that delayed processing of intelligence which results in an actual attack creates far greater audience costs, compared to draconian surveillance practices that are unpopular, but necessary.[58]

However, this dilemma isn't as straightforward as it is discussed in the mainstream, because the debate isn't confined to the realm of state-society relations. Other stakeholders in the debate are foreign intelligence agencies that are competing for information and access, as well as threatening non-state actors from militant groups to hackers.[59] Mass surveillance is becoming a truly global practice, not only because it provides an advantage against terrorist groups and criminal networks, but it also prevents any single intelligence agency to have disproportionate access to surveillance data and establish a global 'digital intelligence monopoly'.[60] The logic is that if a single intelligence agency has the ability to process and store overwhelmingly large volumes of data compared to other agencies, this enables the monopoly agency to weaponize that data in the form of digital espionage or diplomatic strong-arming against other countries. Hence, other agencies expand their surveillance capabilities exponentially to do the same, creating a typical 'security dilemma' in digital space with implications on transparency and secrecy. It is this international intelligence rivalry angle that prevents

[54] Charlie Savage, "Surveillance and Privacy Debate Reaches Pivotal Moment in Congress," The New York Times, January 10, 2018, sec. Politics, https://www.nytimes.com/2018/01/10/us/politics/nsa-surveillance-privacy-section-702-amendment.html.

[55] James Glanz, "Data Centers in Rural Washington State Gobble Power," The New York Times, September 23, 2012, sec. Technology, https://www.nytimes.com/2012/09/24/technology/data-centers-in-rural-washington-state-gobble-power.html.

[56] David Cole and Martin S. Lederman, "The National Security Agency's Domestic Spying Program: Framing the Debate Document," Indiana Law Journal 81 (2006): 1355–1426.

[57] Matthew A. Baum and Tim Groeling, "Shot by the Messenger: Partisan Cues and Public Opinion Regarding National Security and War," Political Behavior 31, no. 2 (June 1, 2009): 157–86, https://doi.org/10.1007/s11109-008-9074-9.

[58] Jeffrey Monaghan and Kevin Walby, "Making up 'Terror Identities': Security Intelligence, Canada's Integrated Threat Assessment Centre and Social Movement Suppression," Policing and Society 22, no. 2 (June 1, 2012): 133–51, https://doi.org/10.1080/10439463.2011.605131.

[59] Julian Richards, "Intelligence Dilemma? Contemporary Counter-Terrorism in a Liberal Democracy," Intelligence and National Security 27, no. 5 (October 1, 2012): 761–80, https://doi.org/10.1080/02684527.2012.708528.

[60] Angela Gendron, "Just War, Just Intelligence: An Ethical Framework for Foreign Espionage," International Journal of Intelligence and CounterIntelligence 18, no. 3 (October 1, 2005): 398–434, https://doi.org/10.1080/08850600590945399.

most governments from engaging in public discussions on digital surveillance.

Yet there are embedded costs of mass surveillance, especially for democratic regimes. Democracies work on the premise of information transparency, where the public has the right to monitor, evaluate and vote for a government's policies.[61] The logic of democracy is that more transparent and better-deliberated policy-making processes have a lower likelihood of failure due to miscalculation and misperception, due to the inclusion of a diverse array of views in the process. Furthermore, because the public and their representatives have greater knowledge and oversight over government practice, democratic governments are also less likely to be able to cover up corruption, mistakes and manipulate statistics, significantly reducing government waste.[62] Authoritarian systems, because they exclude and discourage a great proportion of views from the policy-making process based on ideology or identity, enter into more costly wars, suffer from greater sunk costs and have a greater likelihood of getting entrapped in long-term disputes with their neighbors. Furthermore, because such governments can reliably withhold key policy, spending and appointment information from the public on the grounds of 'national security', these governments tend to be more wasteful in terms of managing human and material capabilities.

Neither democracies nor authoritarian governments can fully forgo either surveillance, or privacy. Even the most transparent governments engage in wide-ranging surveillance practices that are not always fully covered under legal oversight or safeguard mechanisms.[63] Similarly, even the most authoritarian countries have to preserve a semblance of freedom of expression and privacy so that repression doesn't lead to an all-out uprising. What truly separates the surveillance doctrines of democracies and authoritarian regimes on the other hand, is the issue of public consent. In democracies, public can remove leaders who abuse surveillance powers and misuse state secrecy apparatus through free and fair elections; a luxury that the authoritarian regime citizens don't have. Furthermore, democracies possess freedom of information laws that enable citizens to monitor their governments over the long-term, legislative committees that serve as a bridge between the citizens and mechanisms of political secrecy and a protected free press that can establish networks within and around the state secrecy apparatus for sustained public monitoring.

Oversight mechanisms are thus the fundamental locking stone of the privacy-surveillance debate. Such institutions are designed to establish and monitor safeguards with the governments and act as bridges of public consent for surveillance/secrecy policies.[64] They also ensure that an abuse of the government's secrecy monopoly can be punished by the public through audience costs or electoral behavior. Yet the very idea of establishing safeguards against surveillance practices in democracies can be a thorny issue, especially when such democracies are faced with acute national security crises. Canada, Sweden, Norway and the Netherlands for example, have established very strong safeguards that limit the extent of their governments' surveillance powers, whereas United States, France, Greece, Italy and Ireland haven't, largely because of a wide ranging security problems that they deal with. In France, the absence of safeguards has led to wide-ranging skepticism towards post-Bataclan surveillance laws and generated resistance against military service requirements. In the cases of United States and the United Kingdom for example, surveillance agencies' excesses and their ability to hide them from public eye has led to multiple leaks that expressed internal dissent against these wide-ranging powers.

Oversight is a competition between a decision-maker (or a decision group) attempting to make a rapid and payoff maximizing decision that will bolster popularity, status and authority, and the wider civil society aiming to prevent abuse, over-reach and extra-judicial behavior during policy-making. To that end, executives always view oversight as an unnecessary burden that slows down decision-making processes, especially with regard to high-risk and time-constrained events like wars, protests or terrorist attacks. Modern technological advances render the race between surveillance agencies and oversight mechanisms an unfair one, with clear advantage possessed by the former. With improved

[61] Deibert Ronald J. and Rohozinski Rafal, "Risking Security: Policies and Paradoxes of Cyberspace Security," International Political Sociology 4, no. 1 (March 7, 2010): 15–32, https://doi.org/10.1111/j.1749-5687.2009.00088.x.

[62] Colin J. Bennett and David Lyon, eds., Playing the Identity Card: Surveillance, Security and Identification in Global Perspective, 1 edition (London ; New York: Routledge, 2008).

[63] Wilson Matthew C. and Piazza James A., "Autocracies and Terrorism: Conditioning Effects of Authoritarian Regime Type on Terrorist Attacks," American Journal of Political Science 57, no. 4 (June 3, 2013): 941–55, https://doi.org/10.1111/ajps.12028.

[64] Siobhan Gorman, "Reengineering Surveillance Oversight," Lawfare, September 6, 2017, https://www.lawfareblog.com/reengineering-surveillance-oversight.

technological capabilities, agencies are much better able to hide the intricate details of their surveillance practices and the amount of secrets they keep, causing oversight mechanisms to trail back and grow slower over time. Even in a democracy like the UK, weak freedom of information act and slow oversight mechanisms prevent both the public and Prime Minister's Intelligence Security Committee (ISC) to properly understand the scope and depth of GCHQ surveillance practices - a problem which exists in greater proportion in the US.[65]

In the last few years, Canada, Belgium, Croatia, Norway, Sweden and the Netherlands have made significant progress in creating expert, civilian-led oversight bodies that exist alongside national, formal security committees.[66] While most European examples of these independent bodies are made up of all non-elected, public experts, Sweden and Canada created a hybrid independent committee, where technical civilian experts sit alongside legislators. The utility of these independent bodies is a faster delivery of technical detail to legislators themselves, rather than all-legislative committees that are technically not proficient. A helpful, but older standard has been set by the Belgian Standing Intelligence Review Committee, which translated all of its surveillance reports to English and published all its oversight data online for the use of other countries and Belgian citizens.[67] Such data was made public and in English, because the committee believed that surveillance is a transnational problem that could only be resolved through an international, inter-legislative cooperation mechanism.

However just as free and fair elections are rendered meaningful due to the existing of oversight and freedom of information, the reverse is also true: oversight mechanisms can work, only when elections are truly competitive and free. Recent global trends yield a troubling electoral look where democracies that generate illiberal tendencies are increasingly reliant on rigging, gerrymandering or use of implicit threats. For any kind of oversight to work, including digital surveillance oversight, countries have to have meaningful elections and information mechanisms so that the public can reliably monitor and punish governments (either electorally or through audience costs) in cases of abuse.

Conclusion: Privacy versus Secrecy – How Much is Too Much?

How will the society be sure that the decision-makers will use secrecy and surveillance to bolster national security, instead of masking corruption, mismanagement and misjudgment? How can democratic states communicate to the public that the existing surveillance regime is the best middle ground between retaining the country's strategic advantage vis-à-vis rival states, and the society's right to get information about political processes? How can a counter-terrorism chief tell the society that a specific surveillance tactic has reduced the occurrence of terrorist acts, and thereby increase the legitimacy of the program, without revealing the method or avenue to the extremist groups that are targeted? How can the public and/or the parliament be sure that if the counter-terrorism chief reveals the success of the surveillance program, that chief isn't using data selectively to mask the mistakes and abuses of the program?

The answer to these questions are not only difficult, but also cultural – in terms of a country's security, institutional, management and organizational culture. While in some democratic countries, increased secrecy may be viewed as hiding corruption and mismanagement, in others that are faced with direct security threats (cross-border, or terrorist) may view this secrecy as necessary. For example, the French surveillance practices following the Bataclan accounts have been considered over-reach by the voters, and in the absence of the politicians and security chiefs to make a convincing case in favor of the program, public support gradually declined. Such decline had direct repercussions as the voters punished the government by resisting against prolonging military service requirements or purchasing heavy artillery to be used in foreign operations. While intelligence is useful, it cannot on its own mobilize resources for a major conflict or generate favorable public opinion towards supporting allies: governments must win public consent.

The worst practice for a democracy seems to be over-centralizing information, intelligence and national security decisi-

[65] Hayley Evans, "Summary: U.K. Intelligence and Security Committee Annual Report," Lawfare, January 4, 2018, https://www.lawfareblog.com/summary-uk-intelligence-and-security-committee-annual-report.

[66] Zachary K. Goldman and Samuel J. Rascoff, Global Intelligence Oversight: Governing Security in the Twenty-First Century (Oxford: Oxford University Press, 2016).

[67] Nicolas Boring, "Foreign Intelligence Gathering Laws: Belguim," Web page, June 2016, https://www.loc.gov/law/help/intelligence-activities/belguim.php.

ons into a small group of decision-makers, without establishing accountability mechanisms. This generates long-term doubt about key policy issues, creates permanent public resistance against such political overtures and sap the country's foreign policy efforts – even when such voices cannot find space in the mainstream. Such resistance will significantly increase once extra-judicial conflict practices, such as torture, or civilian killings become exposed ex-post, as a result of leaks.

Good democratic practice on the other hand, includes a degree of oversight and safeguards; both how much? Michael Colaresi argues in favor of a 'time lag'.[68] In the time lag model, the state reveals policy that requires public consent gradually, over time, in order to retain the immediate secrecy of the policy in question, but then opening it up to public discussion and consent within a reasonable time frame. It is usually the secrets that remain so for an extended period of time (sometimes indefinitely) that generate some of the core debates in the privacy-surveillance debate. Second, 'retrospective accountability' mechanisms have to be set in place, so that those who abuse national secrecy will at some point face the consequences of such over-reach. To do that, reliable archival infrastructure has to be in place, along with institutional processes that can reliably go back in time to introduce most of the concealed documents or evidence with the public. Legislative and legal oversight has to be sufficiently strong so that once the time lag of secrecy has expired, both institutions can reasonably evaluate what the executive has done under secrecy. Democracies always have strong institutions that safeguard and oversee the use of secrecy during emergencies, and to incur costs on the leaders retrospectively, perhaps late, but with definite eventuality.

Such mechanisms don't exist in autocracies, as neither the legislative, nor the legal oversight options can reliably incur any weight on the over-reaching executive, even long after the expiration of the time lag. Although this may seem to be a good scenario for autocratic leaders, it is also a lonely one in which public support for policies are always lower than it could be under more representative conditions and also lonely in terms of the decision-making cohort into which only political appointees are allowed. In crisis scenarios, such as war, civil unrest, or overseas military involvement, leaders are forced to mobilize the greatest amount of national resources (monetary, technological, manpower and human quality) to perform well in the said emergency. Once decision-making on these issues are shrouded into a thick fog of mystery, which is equally thick for domestic and international audiences, then the process leaves out great portions of these national resources, forcing the leader to make fast, unitary decision, but ones that punch below the country's weight. In addition, once the society ends up unconvinced about why the state employs draconian digital surveillance measures and conducts active spying on civilians, the force of the resistance becomes even stronger.

Ultimately, democracies have to come up with the surveillance-privacy balance that conforms to the country's political culture, but also to the universal human rights. The task of oversight in this context is heavy: it has to continuously chase the executive and intelligence community in detecting abuse and excess, while remaining technologically proficient at the same time. Most of the time when oversight mechanisms don't work, this happens due to such mechanisms growing technically obsolete, or unable to understand newer technologies through which surveillance and monitoring is conducted. Digital surveillance oversight has to balance between an impetuous executive that seeks to engage in power-maximizing behavior, and an inquisitive public, which is interested in preventing corruption, mismanagement and abuse. Executive and security-intelligence communities will naturally seek to avoid oversight and the public will always have a maximalist understanding of transparency that will remain unrealistic given states' security dilemma problems. Oversight mechanisms will fail to balance if they fall behind the technological developments in surveillance-privacy field or take too long to monitor the process of secrecy. This means that just like in offline democracy, online democracy is only as strong as its oversight mechanisms and safeguards.

[65] Colaresi;, Democracy Declassified.

References

Altheide, David L. "The Triumph of Fear: Connecting the Dots about Whistleblowers and Surveillance." *International Journal of Cyber Warfare and Terrorism (IJCWT)* 4, no. 1 (January 1, 2014): 1–7. https://doi.org/10.4018/ijcwt.2014010101.

Ball, Kirstie, and Laureen Snider. *The Surveillance-Industrial Complex: A Political Economy of Surveillance.* New York: Routledge, 2013.

Baum, Matthew A., and Tim Groeling. "Shot by the Messenger: Partisan Cues and Public Opinion Regarding National Security and War." *Political Behavior* 31, no. 2 (June 1, 2009): 157–86. https://doi.org/10.1007/s11109-008-9074-9.

BBC/Panorama, Source: "Edward Snowden: GCHQ Wants to Own Your Phone – Video." *The Guardian*, October 5, 2015, sec. US news. http://www.theguardian.com/us-news/video/2015/oct/05/edward-snowden-gchq-wants-own-your-phone-video.

Bennett, Colin J., and David Lyon, eds. *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective.* 1 edition. London ; New York: Routledge, 2008.

Bennett, Colin J., and Charles D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective.* New York: Routledge, 2017.

Bentham, Jeremy. *Panopticon: The Inspection House.*CreateSpace Independent Publishing Platform, 2017.

Blum, Stephanie Cooper. "What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform." *Boston University Public Interest Law Journal* 18 (2009 2008): 269–314.

Boring, Nicolas. "Foreign Intelligence Gathering Laws: Belguim." Web page, June 2016. https://www.loc.gov/law/help/intelligence-activities/belguim.php.

———. "Foreign Intelligence Gathering Laws: France | Law Library of Congress." Web page, December 2014. https://www.loc.gov/law/help/foreign-intelligence-gathering/france.php.

Born, Dr Hans, and Ms Marina Caparini. *Democratic Control of Intelligence Services: Containing Rogue Elephants.* Ashgate Publishing, Ltd., 2013.

Botsman, Rachel. "Big Data Meets Big Brother as China Moves to Rate Its Citizens." WIRED UK, October 2017. http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion.

Bullingham, Liam, and Ana C. Vasconcelos. "'The Presentation of Self in the Online World': Goffman and the Study of Online Identities." *Journal of Information Science* 39, no. 1 (February 1, 2013): 101–12. https://doi.org/10.1177/0165551512470051.

Carey, Scott. "Investigatory Powers Act: What You Need to Know." ComputerworldUK, January 2018. https://www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/.

Chadwick, Andrew, and Philip N. Howard. *Routledge Handbook of Internet Politics.* Taylor & Francis, 2010.

Chang, Alvin. "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram." Vox, March 23, 2018. https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

"China Passes Tough New Intelligence Law." *Reuters*, June 28, 2017. https://www.reuters.com/article/us-china-security-lawmaking/china-passes-tough-new-intelligence-law-idUSKBN19I1FW.

Colaresi;, Michael P. *Democracy Declassified: The Secrecy Dilemma in National Security by Michael P. Colaresi.* Oxford University Press, 2014.

Cole, David, and Martin S. Lederman. "The National Security Agency's Domestic Spying Program: Framing the Debate Document." *Indiana Law Journal* 81 (2006): 1355–1426.

Davis, Robert N. "Striking the Balance: National Security vs. Civil Liberties." *Brooklyn Journal of International Law* 29 (2004 2003): 175–238.

De Capitani Di Vimercati, Sabrina, Sara Foresti, Giovanni Livraga, and Pierangela Samarati. "Data Privacy: Definitions and Techniques." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 20, no. 6 (December 1, 2012): 793–817. https://doi.org/10.1142/S0218488512400247.

Deibert Ronald J., and Rohozinski Rafal. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology* 4, no. 1 (March 7, 2010): 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x.

Donohue, Laura K. *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*. Oxford: Oxford University Press, 2016.

Evans, Hayley. "Summary: U.K. Intelligence and Security Committee Annual Report." Lawfare, January 4, 2018. https://www.lawfareblog.com/summary-uk-intelligence-and-security-committee-annual-report.

Fischer-Hbner, Simone, and Stefan Berthold. "Chapter 43 - Privacy-Enhancing Technologies1." *In Computer and Information Security Handbook (Second Edition)*, edited by John R. Vacca, 755–72. Boston: Morgan Kaufmann, 2013. https://doi.org/10.1016/B978-0-12-394397-2.00043-X.

Foucault, Michel. *Discipline & Punish: The Birth of the Prison*. Translated by Alan Sheridan. New York: Vintage Books, 1995.

Gangadharan, Seeta Peña. "The Downside of Digital Inclusion: Expectations and Experiences of Privacy and Surveillance among Marginal Internet Users." New Media & Society 19, no. 4 (April 1, 2017): 597–615. https://doi.org/10.1177/1461444815614053.

Gendron, Angela. "Just War, Just Intelligence: An Ethical Framework for Foreign Espionage." *International Journal of Intelligence and CounterIntelligence* 18, no. 3 (October 1, 2005): 398–434. https://doi.org/10.1080/08850600590945399.

Gesley, Jenny. "Foreign Intelligence Gathering Laws: Germany." Web page, June 2016. https://www.loc.gov/law/help/intelligence-activities/germany.php.

Gibbs, Samuel. "What Is 'Safe Harbour' and Why Did the EUCJ Just Declare It Invalid?" the Guardian, October 6, 2015. http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection.

Glanz, James. "Data Centers in Rural Washington State Gobble Power." *The New York Times*, September 23, 2012, sec. Technology. https://www.nytimes.com/2012/09/24/technology/data-centers-in-rural-washington-state-gobble-power.html.

Goad, Ben. "New Pressure on US Tech to Comply with China's Access Demands." Text. TheHill, October 16, 2015. http://thehill.com/policy/cybersecurity/257194-new-pressure-on-us-tech-to-comply-with-chinas-access-demands.

Goldman, Zachary K., and Samuel J. Rascoff. *Global Intelligence Oversight: Governing Security in the Twenty-First Century*. Oxford: Oxford University Press, 2016.

Gorman, Siobhan. "Reengineering Surveillance Oversight." Lawfare, September 6, 2017. https://www.lawfareblog.com/reengineering-surveillance-oversight.

Greenwald, Glenn, and Spencer Ackerman. "How the NSA Is Still Harvesting Your Online Data." the Guardian, June 27, 2013. http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

"Hacker Lexicon: What Is a Backdoor?" WIRED. Accessed March 28, 2018. https://www.wired.com/2014/12/hacker-lexicon-backdoor/.

Hern, Alex. "Strava Suggests Military Users 'Opt Out' of Heatmap as Row Deepens." the Guardian, January 29, 2018. http://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban.

Himmelfarb, Gertrude. *The Roads to Modernity: The British, French, and American Enlightenments*. Reprint edition. New York New York: Vintage, 2005.

Landau, S. "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations." *IEEE Security Privacy* 11, no. 4 (July 2013): 54–63. https://doi.org/10.1109/MSP.2013.90.

Langner, R. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security Privacy* 9, no. 3 (May 2011): 49–51. https://doi.org/10.1109/MSP.2011.67.

Lee, Dave. "China and US Clash over Backdoors." *BBC News*, March 4, 2015, sec. Technology. http://www.bbc.com/news/technology-31729305.

Ling, Justin. "The Story of How Canadian Police Committed Arson to Stop a Black Panther Meeting." VICE News, June 2017. https://news.vice.com/en_ca/article/eva8da/story-of-how-canadian-police-committed-arson-to-stop-a-black-panther-meeting.

Luhn, Alec. "Russia Passes 'Big Brother' Anti-Terror Laws." the Guardian, June 26, 2016. http://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws.

Lütticke, Marcus. "New Leaks Show Germany's Collusion with NSA | DW | 21.06.2014." DW.COM, June 2014. http://www.dw.com/en/new-leaks-show-germanys-collusion-with-nsa/a-17726141.

Lyon, David, Kirstie Ball, and Kevin D. Haggerty. *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012.

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications." the Guardian, June 21, 2013. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

Marx Gary T. "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance." *Journal of Social Issues* 59, no. 2 (April 29, 2003): 369–90. https://doi.org/10.1111/1540-4560.00069.

McCoy, Damon, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. "Shining Light in Dark Places: Understanding the Tor Network." *In Privacy Enhancing Technologies*, 63–76. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2008. https://doi.org/10.1007/978-3-540-70630-4_5.

Meister, Andre. "How the German Foreign Intelligence Agency BND tapped the Internet Exchange Point DE-CIX in Frankfurt, since 2009." *netzpolitik.org* (blog), March 31, 2015. https://netzpolitik.org/2015/how-the-german-foreign-intelligence-agency-bnd-tapped-the-internet-exchange-point-de-cix-in-frankfurt-since-2009/.

Miller, Jacques-Alain, and Richard Miller. "Jeremy Bentham's Panoptic Device." *October* 41 (1987): 3–29. https://doi.org/10.2307/778327.

Mitchell, Anna, and Larry Diamond. "China's Surveillance State Should Scare Everyone." *The Atlantic*, February 2, 2018. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/.

Monaghan, Jeffrey, and Kevin Walby. "Making up 'Terror Identities': Security Intelligence, Canada's Integrated Threat Assessment Centre and Social Movement Suppression." *Policing and Society* 22, no. 2 (June 1, 2012): 133–51. https://doi.org/10.1080/10439463.2011.605131.

Mou, Yi, Kevin Wu, and David Atkin. "Understanding the Use of Circumvention Tools to Bypass Online Censorship." *New Media & Society* 18, no. 5 (May 1, 2016): 837–56. https://doi.org/10.1177/1461444814548994.

Pacis, Jessamine. "State of Surveillance in the Philippines." *Foundation for Media Alternatives* (blog), April 7, 2016. https://www.fma.ph/2016/04/07/state-of-surveillance-in-the-philippines/.

Phillips, Tom. "China Testing Facial-Recognition Surveillance System in Xinjiang – Report." the Guardian, January 18, 2018. http://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report.

Privacy International. "A New Era of Mass Surveillance Is Emerging Across Europe." *Medium* (blog), January 17, 2017. https://medium.com/privacy-international/a-new-era-of-mass-surveillance-is-emerging-across-europe-3d56ea35c48d.

Richards, Julian. "Intelligence Dilemma? Contemporary Counter-Terrorism in a Liberal Democracy." *Intelligence and National Security* 27, no. 5 (October 1, 2012): 761–80. https://doi.org/10.1080/02684527.2012.708528.

Rosen, Jeffrey. "The Right to Be Forgotten Symposium Issue: The Privacy Paradox: Privacy and Its Conflicting Values." *Stanford Law Review Online* 64 (2012 2011): 88–92.

Savage, Charlie. "Surveillance and Privacy Debate Reaches Pivotal Moment in Congress." *The New York Times*, January 10, 2018, sec. Politics. https://www.nytimes.com/2018/01/10/us/politics/nsa-surveillance-privacy-section-702-amendment.html.

Soldatov, Andrei, and Irina Borogan. "Inside the Red Web: Russia's Back Door onto the Internet – Extract." the Guardian, September 8, 2015. http://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet.

Wang, Yang. "Privacy-Enhancing Technologies." *Handbook of Research on Social and Organizational Liabilities in Information Security*, 2009, 203–27. https://doi.org/10.4018/978-1-60566-132-2.ch013.

Willsher, Kim. "France Approves 'Big Brother' Surveillance Powers despite UN Concern." the Guardian, July 24, 2015. http://www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers.

Wilson Matthew C., and Piazza James A. "Autocracies and Terrorism: Conditioning Effects of Authoritarian Regime Type on Terrorist Attacks." *American Journal of Political Science* 57, no. 4 (June 3, 2013): 941–55. https://doi.org/10.1111/ajps.12028.

Wong, Cynthia. "Big Brother Is Watching: Why We Should Fear Surveillance in the New World Order." Newsweek, February 7, 2017. http://www.newsweek.com/state-surveillance-europe-populism-cctv-citizens-553857.

Cyber Governance and Digital Democracy 2018/2

April 2018

Politics of Digital Surveillance, National Security and Privacy

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has University