Cambridge University Press
978-1-107-18110-6 — The Cambridge Handbook of Consumer Privacy
Edited by Evan Selinger , Jules Polonetsky , Omer Tene
Excerpt
More Information

PART I

Introduction

1

Consumer Privacy and the Future of Society

Jules Polonetsky, Omer Tene, and Evan Selinger

In the course of a single day, hundreds of companies collect massive amounts of information from individuals. Sometimes they obtain meaningful consent. Often, they use less than transparent means. By surfing the web, using a cell phone and apps, entering a store that provides Wi-Fi, driving a car, passing cameras on public streets, wearing a fitness device, watching a show on a smart TV or ordering a product from a connected home device, people share a steady stream of information with layers upon layers of hardware devices, software applications, and service providers. Almost every human activity, whether it is attending school or a workplace, seeking healthcare or shopping in a mall, driving on a highway or watching TV in the living room, leaves behind data trails that build up incrementally to create a virtual record of our daily lives. How companies, governments, and experts should use this data is among the most pressing global public policy concerns.

Privacy issues, which are at the heart of many of the debates over data collection, analysis, and distribution, range extensively in both theory and practice. In some cases, conversations about privacy policy focus on marketing issues and the minutiae of a website's privacy notices or an app's settings. In other cases, the battle cry for privacy extends to diverse endeavors, such as the following: calls to impose accountability on the NSA's counterterrorism mission;[1] proposals for designing safe smart toys;[2] plans for enabling individuals to scrub or modify digital records of their pasts;[3] pleas to require database holders to inject noise into researchers' queries to protect against leaks that disclose an individuals' identity;[4] plans to use crypto currencies[5] or to prevent criminals and terrorists from abusing encryption tools;[6] proposals for advancing medical research

[1] Richard Clarke, Michael Morell, Geoffrey Stone, Cass Sunstein & Peter Swire, The NSA Report: Liberty and Security in a Changing World (The President's Review Group on Intelligence and Communications Technologies, Princeton University Press, 2014).

[2] *Kids and the Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots* (Future of Privacy Forum and Family Online Safety Institute, Dec. 2016), https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf.

[3] Case C-131/12 Google Spain v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI: EU:C:2014:317.

[4] Cynthia Dwork, Frank McSherry, Kobbi Nissim & Adam Smith, *Calibrating Noise to Sensitivity in Private Data Analysis*, in Proceedings of the 3rd Theory of Cryptography Conference, 265–284 (2006).

[5] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller & Steven Goldfeder, Bitcoin and Cryptocurrency Technologies (Princeton University Press, 2016).

[6] In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 15-mc-1902 (JO) (E.D.N.Y. Feb. 29, 2016).

and improving public health without sacrificing patients' control over their data;[7] and ideas for how scientists can make their data more publicly available to facilitate replication of studies without, at the same time, inadvertently subjecting entire populations to prejudicial treatment, including discrimination.[8]

At a time when fake news influences political elections, new and contentious forms of machine-to-machine communications are emerging, algorithmic decision-making is calling more of the shots in civic, corporate, and private affairs, and ruinous data breaches and ransomware attacks endanger everything from financial stability to patient care in hospitals, "privacy" has become a potent shorthand. Privacy is a boundary, a limiting principle, and a litmus test for identifying and adjudicating the delicate balance between the tremendous benefits and dizzying assortment of risks that insight-filled data offers.

DIVERSE PRIVACY PERSPECTIVES

The wide scope of perspectives found in this collection reflects the very diversity of privacy discourse.

Since privacy is front-page news, politicians regularly weigh in on it. Some politicians make privacy their signature issue by submitting legislative proposals, convening committee hearings, and sending letters to technology companies as they launch and test new tools. Interestingly, in the United States, privacy can be a bipartisan issue that brings together coalitions from opposite sides of the aisle. For example, on questions of national security surveillance, right wing libertarians side with left wing civil rights activists in opposing government powers and advocating for robust oversight mechanisms. However, in the consumer privacy space, traditional roles are often on display as supporters of regulation spar with free market activists on issues ranging from telecom regulation to the legitimacy of the data broker industry. In Europe, left wing parties, such as the German Greens or the Scandinavian Pirate Party, have played important roles in privacy advocacy by embracing an expansive reading of data protection principles. Conservatives, by contrast, have sought to balance data protection against economic interests and free trade. This political tension manifests itself in the twin, often conflicting objectives of the European data protection regime, which instructs Member States to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data," while, at the same time, "neither restrict[ing] nor prohibit [ing] the free flow of personal data between Member States."

Industry interest in privacy often aligns with businesses uniformly vying for more data use and less regulation. Even so, opinions still splinter across a broad spectrum. Some publishers believe that stronger limits on ad-tracking will advantage them to collect ad revenue that is earned today by advertising technology companies or large platforms. Other companies believe that new data portability rules will enable them to leverage data now held by platforms to better compete or to launch new services. Nevertheless, incumbents in many sectors worry that new regulations and more extensive liability will impede their digital strategies.

[7] Salil Vadhan, David Abrams, Micah Altman, Cynthia Dwork, Paul Kominers, Scott Duke Kominers, Harry Lewis, Tal Moran & Guy Rothblum, Comments on Advance Notice of Proposed Rulemaking: Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, Docket ID No. HHS-OPHS-2011–0005 (2011), https://privacytools.seas.harvard.edu/publications/comments-advance-notice-proposed-rulemaking-human-subjects-research.

[8] Daniel Goroff, Jules Polonetsky & Omer Tene, *Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data*, 65 Ann. Am. Acad. Pol. & Soc. Sci. 46–66 (2018).

Regulators chase the flurry of market developments with carrots and sticks. Approaches vary, with some regulators, such as the UK Information Commissioner's Office, offering advice, best practices, and compliance tools. Others, such as the Canadian Federal Privacy Commissioner, enhance limited enforcement powers by actively engaging with the media to "name and shame" alleged violations of privacy laws. Some European data protection regulators are known to levy stiff fines and penalties even for technical violations of local statutes. The compliance risks for businesses will escalate sharply with the imposition of formidable sanctions under the General Data Protection Regulation. The Federal Trade Commission (FTC), the main federal privacy regulator in the United States, has developed a complex privacy and security regulatory approach that is built on two pillars. On the one hand, it includes a string of settlements referred to by Daniel Solove and Woodrow Hartzog as a "common law" of privacy.[9] On the other hand, the FTC issues a line of policy guidelines through workshops and reports on cutting-edge issues ranging from connected vehicles and consumer genetics to the sharing economy.

Privacy academics are a heterogeneous group who occupy a central place in policy debates. Some are data optimists. They see a bright future in data-intensive technologies and seek to facilitate their adoption while respecting individuals' rights. Others are data pessimists. They warn against the disruptive risk of data technologies and in extreme cases even see an inevitable decline toward a "database of ruin."[10] More traditionally, academics can be loosely categorized according to their disciplines. Law and policy scholars explore issues such as the Fourth Amendment, privacy legislation such as the Health Insurance Portability Act, the Family Educational Rights and Privacy Act, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act, and the FTC's body of privacy law. Computer scientists deal with issues such as security and privacy in online, mobile operating systems and software, network security, anonymity, human–machine interaction, and differential privacy. Engineers work on network security, values in design, privacy by design, blockchain, and privacy-enhancing technologies. Economists assess the value and markets for data, as well as such issues as the value of privacy, privacy incentives and nudges, data-based price discrimination, privacy in credit and health markets, the behavioral economics of privacy, and more. Design schools innovate privacy messaging, information schools explore the role of privacy in media and culture, psychologists experiment on individuals' responses to incentives in cyber and real-world spaces, and ethicists weigh in on all of this.

CONSUMER PRIVACY

This book brings together academics, policy makers, and industry leaders to critically address the subset of issues that are raised in the context of *consumer privacy*. It purposefully sets aside the fateful dilemmas raised by government surveillance. This includes the continuing fallout from Edward Snowden's revelations about the prevalence of government access to private communications data. And it extends to newly emerging challenges, such as deploying military drones to assassinate suspected terrorists, using data-driven software for criminal sentencing, and monitoring people awaiting trial and serving court-mandated sentences in the seclusion of their homes. Yet, even narrowed to consumer privacy, this book still addresses a rich spectrum of issues triggered by an exceedingly broad swath of activities. While consumer privacy once was limited

[9] Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).
[10] Paul Ohm, *Don't Build a Database of Ruin*, HARV. BUS. REV, Aug. 23, 2012, https://hbr.org/2012/08/dont-build-a-database-of-ruin.

to the realm of online tracking for targeted advertising,[11] the topic now extends to wearable technologies and implantable medical devices, smart homes and autonomous vehicles, facial recognition and behavioral biometrics, and algorithmic decision-making and the Internet of Things.[12] As companies collect massive amounts of data through the Internet, mobile communications, and a vast infrastructure of devices and sensors embedded in healthcare facilities, retail outlets, public transportation, social networks, workplaces, and homes, they use the information to test new products and services, improve existing offerings, and conduct research.

Given the wide scale and scope of consumer privacy, the topic can't be easily distinguished from government surveillance. With companies amassing huge warehouses of personal information, governments can swoop in when necessary to access the data through procurement, legal process, or technological capabilities. As Chris Hoofnagle observed more than a decade ago, "Accumulations of information about individuals tend to enhance authority by making it easier for authority to reach individuals directly. Thus, growth in society's record-keeping capability poses the risk that existing power balances will be upset."[13]

Since each new space and field of activity raises weighty policy, legal, ethical, economic, and technological questions and challenges, input on privacy is needed from experts across the disciplines. Philosophers, social scientists, legal theorists, geneticists, mathematicians, computer scientists, and engineers all have important roles to play. The pressing debates require a careful balancing of diverse values, interests, rights, and considerations. In many cases, individual benefits are pitted against the public good, and this tension tests the contours of autonomy and fundamental human rights in a constantly shifting techno-social environment.

The impact of technology on the economy and global markets cannot be overstated. Several of the most highly valued companies are data-driven innovators. That is why companies such as Apple, Google, Microsoft, Amazon, and Facebook, alongside traditional technology powerhouses, such as Intel, IBM and AT&T, and new upstarts, including Uber and Snap, are the focus of heated consumer discussion and regulatory debate.[14] This trend goes beyond the United States and, more broadly, the Western world. Chinese tech giants, such as Baidu, Alibaba, JD.com, and surging new entrants – notably, Didi Chuxing, and Lu.com – are shaking up the Asian economy and gaining a global footprint.[15] These companies have profound impacts our lives. Every day, they confront a host of complex value-laden choices when designing products that collect, analyze, process, and store information about every aspect of our behavior. Realizing the magnitude of these decisions, companies have begun to create ethical review processes, employ data ethicists and philosophers, and seek guidance from academics, think tanks, policymakers, and regulators.[16] The role of the chief privacy officer, once the domain of only a handful of

[11] Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 Minn. J. L. Sci. & Tech. 281 (2012).

[12] Woodrow Hartzog & Evan Selinger, *The Internet of Heirlooms and Disposable Things*, 17 N. C. J. L. & Tech. 581 (2016).

[13] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement*, 29 N. C. J. Int'l L. & Com. Reg. 595 (2004).

[14] Farhad Manjoo, Tech's *"Frightful 5" Will Dominate Digital Life for Foreseeable Future*, N.Y. Times, Jan. 20, 2016, https://www.nytimes.com/2016/01/21/technology/techs-frightful-5-will-dominate-digital-life-for-foreseeable-future.html.

[15] Brendon Kochkodin, *Chinese Big Five Tech Companies Gain on U.S. Counterparts*, Bloomberg Businessweek, June 22, 2017, https://www.bloomberg.com/news/articles/2017-06-23/chinese-big-five-tech-companies-gain-on-u-s-counterparts.

[16] Jules Polonetsky, Omer Tene & Joseph Jerome, *Beyond the Common Rule: Ethical Structures for Data Research in Non-Academic Settings*, 13 Colo. Tech. L. J. 333 (2015); also see Ryan Calo, *Consumer Subject Review Boards: A Thought Experiment*, 66 Stan. L. Rev. Online 97, 102 (2013); Evan Selinger & Woodrow Hartzog, *Facebook's*

technology leaders, has emerged as a strategic C-suite position.[17] Within a decade, privacy has matured into a full-fledged profession with a body of knowledge, professional certifications, and formal legal status.[18]

Increasingly, not only companies but also government entities are transforming into data service providers for consumers. Consider smart cities, where local governments have become hubs of data that is collected through growing networks of sensors and connected technologies to generate actionable, often real-time information.[19] By relying on ubiquitous telecommunications technologies to provide connectivity to sensor networks and set actuation devices into operation, smart cities are increasingly collecting information on cities' air quality, temperature, noise, street and pedestrian traffic, parking capacity, distribution of government services, emergency situations, and crowd sentiments, among other data points. This information can now be cheaply aggregated, stored, and analyzed to draw conclusions about the intimate affairs of city dwellers. The more connected a city becomes, the more it will generate steady streams of data from and about its citizens and the environment they live in.[20]

The urban data revolution enables cities to better manage traffic congestion, improve energy efficiency, expand connectivity, reduce crime, and regulate utility flow. By analyzing data trends and auditing the performance of schools, public transportation, waste management, social services, and law enforcement, smart cities can better identify and respond to discriminatory practices and biased decision-making, empowering weakened populations and holding institutions to account. At the same time, the specter of constant monitoring threatens to upset the balance of power between city governments and city residents. At the extreme, it might destroy the sense of anonymity that has defined urban life over the past century. As Kelsey Finch and Omer Tene observe, "There is a real risk that, rather than standing as 'paragons of democracy,' [smart cities] could turn into electronic panopticons in which everybody is constantly watched."[21]

Smart community policy also highlights the tension between the push for open data mandates and public records acts and the desire citizens have for privacy. On the one hand, the transparency goals of the open data movement serve important social, economic, and democratic functions. Open and accessible public data can benefit individuals, companies, communities, and government by fueling new social, economic, and civic innovations, and improving government accountability and transparency. On the other hand, because the city collects and shares information about its citizens, public backlash over intrusive surveillance remains an ever-present possibility.[22] Due to these competing concerns, the consumer privacy discussion requires aligning potentially conflicting interests: maximizing transparency and accountability without forsaking individual rights.

Emotional Contagion Study and the Ethical Problem of Co-Opted Identity in Mediated Environments Where Users Lack Control, 12 Research Ethics 35 (2016).

[17] Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 Ohio St. L. J. 897 (2013).

[18] J. Trevor Hughes & Cobun Keegan, *Enter the Professionals: Organizational Privacy in a Digital Age* (see Chapter 22).

[19] Kelsey Finch & Omer Tene, *Welcome to Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 Fordham Urban L. J. 1581 (2015).

[20] Kelsey Finch & Omer Tene, *The City as a Platform: Enhancing Privacy and Transparency in Smart Communities* (see Chapter 7).

[21] Finch & Tene, *supra* note 16, at 1583.

[22] Ben Green, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer & Susan Crawford, *Open Data Privacy: A Risk-Benefit, Process-Oriented Approach to Sharing and Protecting Municipal Data* (Berkman Klein Center for Internet & Society Research Publication, 2017), https://dash.harvard.edu/bitstream/handle/1/30340010/OpenDataPrivacy.pdf.

BEYOND PRIVACY

As we have been suggesting, arguments about privacy have become proxy debates for broader societal choices about fairness, equity, and power. Since data is central to economic activity across every sector – government, non-profit, and corporate – the privacy debate has spilled over to adjacent areas. Educational technology is a prime example.

Long confined to using textbooks, blackboards, and pencil-and-paper testing, schools now use new applications, hardware, and services. This includes online curricula and tools, social media and cloud applications for file sharing and storage, note taking, and collaboration platforms, and a variety of connected tablets and workstations. Student performance data is driving next-generation models of learning and measurements for teacher effectiveness. And connected learning is fast becoming a path for access to knowledge and academic achievement.

New educational technology offers many advantages for educators, teachers, parents, and students. Education has become more interactive, adaptive, responsive, and even fun. Parents can stay apprised of their child's performance, accomplishments, and difficulties without weighing down teachers' limited time resource. Teachers can connect to sophisticated learning management systems, while school administrations can obtain rich, measurable inputs to better calibrate resources to needs.[23]

However, from a privacy perspective, the confluence of enhanced data collection that contains highly sensitive information about children and teens also makes for a combustive mix. New data flows raise questions about who should have access to students' data and what are the legitimate uses of the information. Should a developer of a math app be authorized to offer high-performing students a version that covers more advanced material, or would that be considered undesirable marketing to children? Should an educational social network be permitted to feature a third-party app store for kids? Or, if an education service detects a security vulnerability on a website that is available for schools to use, should it be able to leverage its knowledge to protect schools as well as clients outside of the educational sector? And what about education technology developers who want to use the data they extract from students to develop software for the general market?

It is clear that when it comes to education, privacy means different things to different people and traditional privacy problems are only the tip of the policy iceberg. Activists have challenged data collection and use to debate school reform, common core curricula, standardized testing, personalized learning, teacher assessments, and more. Some critics even consider efforts to ramp up education technology misguided altogether, labeling them as the work of "corporate education reformers" who seek profit at the expense of public education. Ultimately, then, the challenge for educational technology entails differentiating problems that can be remedied with privacy solutions from problems that require other resolutions because they are, at bottom, proxies for conflicts about education policy.

Complex conversations also surround smart cars and autonomous vehicles. On the one hand, collecting data in cars is old hat. Vehicles have had computerized data systems since the 1960s. On the other hand, things are profoundly changing now that vehicles are becoming data hubs that collect, process, and broadcast information about drivers' performance, geolocation, telematics, biometrics, and even media consumption. Furthermore, vehicle-to-vehicle (V2V)

[23] Jules Polonetsky & Omer Tene, *Who is Reading Whom Now: Privacy in Education from Books to MOOCs*, 17 Vand. J. Ent. & Tech. L. 927 (2015); *also see* Jules Polonetsky & Omer Tene, *The Ethics of Student Privacy: Building Trust for Ed Tech*, 21 Int'l Rev. Info. Ethics 25 (2014).

technology introduces a new way for smart cars to seamlessly receive and analyze information about other vehicles. This capability is essentially transforming public thoroughfares into a seamless network of information about each vehicle's position, direction of travel, speed, braking, and other variables that telematics studies.[24]

Smart car data collection raises all kinds of issues. Consumers and advocates are concerned about cars extracting personal data that can be shared with government and law enforcement. Security experts are anxious about self-driving cars being vulnerable to hacking. At the same time, under the banner of privacy concerns, critics also discuss ethics, labor markets, insurance premiums, and tradeoffs between safety and autonomy. For example, while smart cars and autonomous vehicles can reduce traffic accidents, they will also need to make decisions with moral implications, such as choosing to prioritize the safety of passengers or pedestrians. Coding algorithms to make momentous moral choices is a formidable challenge that transcends the guidance traditional privacy frameworks offer.

Insurance companies are vigorously embracing the growth in vehicle-generated data by developing usage-based applications to harness information emanating from onboard diagnostic systems. These applications provide insurers with information on how a vehicle is driven, and they factor in this information when making decisions about safe driver programs and personalized insurance rates. While the Fair Credit Reporting Act applies to the process of using data to make insurance decisions, its standards cannot address all of the questions that are starting to arise. Concern is being expressed over allocations of risk and the process of creating categories of drivers who are uninsurable due to traits and tendencies that potentially can be correlated with health, genetics, race, and ethnicity. Also, within a generation, autonomous vehicles will fundamentally upend labor markets. Ostensibly consumers will benefit from increased fleet efficiency and huge savings in labor costs. At the same time, the economic changes seem poised to dramatically affect employment prospects, especially for the millions of taxi and truck drivers in the United States and beyond.[25] These policy issues clearly extend digital and cyber privacy debates into new realms and possibly transform them as well.

THE FUTURE OF SOCIETY

The upshot of the dynamics and processes highlighted here is that the chapters in this book are about much more than consumer privacy – which is to say, they go far beyond consumer privacy construed as a niche topic. Contributors fundamentally advance conversations about what paths should be paved in order to create flourishing societies in the future. With every aspect of human behavior being observed, logged, analyzed, categorized, and stored, technology is forcing legislatures, regulators, and courts to deal with an incessant flow of weighty policy choices. These debates have long spilled over from the contours of privacy, narrowly defined as a right to anonymity, seclusion and intimacy – a right to be let alone[26] – to a discussion about power and democracy, social organization, and the role humans should occupy in technologically mediated spaces. These tough discussions are about matters such as exposure, profiling and discrimination, self-expression, individual autonomy, and the relative roles of humans and machines.

[24] Lauren Smith & John Verdi, *Comments from the Future of Privacy Forum to the Federal Trade Commission and U.S. Department of Transportation* (National Highway Traffic Safety Administration, May 1, 2017), https://fpf.org/wp-content/uploads/2017/05/Future-of-Privacy-Forum-Comments-FTC-NHTSA-Workshop.pdf.

[25] *See, e.g.*, *The Future of Jobs: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution* (World Economic Forum, Jan. 2016), http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf.

[26] Samuel Warren and & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

Consider what happened when a teacher was fired after a picture was posted on Facebook of her dressed as a drunk pirate. It was hard to know if the ensuing public debate was about privacy settings on the social network or the limits of assessing behavior in a world where every action is documented, tagged, and presented to the public to judge.[27] Similarly, it is hard to pinpoint what parents and teachers are concerned about when they recoil against ephemeral cyberbullying messages on apps such as Snapchat. Is it dismay about the software's privacy settings? Or might it be sadness over the cruel experiences of childhood being exposed and augmented through a new medium?[28] And what about autonomous vehicles engineers who design a real-life response to the longstanding trolley problem? Are they dealing with fair information practice principles or ethical challenges that have occupied philosophers from Aristotle to Immanuel Kant and John Stuart Mill?[29]

Advances in artificial intelligence and machine learning keep raising the stakes. Developers deploy artificial intelligence to improve organizations' performance and derive predictions in almost every area of the economy. This happens in domains ranging from social networks, autonomous vehicles, drones, precision medicine, and the criminal justice system. And it includes such processes as speech and image recognition, universal translators, and ad targeting, to name a few. Organizations leverage algorithms to make data-based determinations that impact individuals' rights as citizens, employees, seekers of credit or insurance, and so much more. For example, employers use algorithms to assess prospective employees by offering neuroscience-based games that are said to measure inherent traits. Even judges turn to algorithms for sentencing and parole decisions. They use data to predict a person's risk of recidivism, violence, or failure to appear in court based on a complicated mix of behavioral and demographic characteristics.[30]

Daniele Citron has written about the importance of creating appropriate standards of algorithmic due process that include transparency, a right to correct inaccurate information, and a right to appeal adverse decisions.[31] Unfortunately, this goal might be incredibly difficult to meet. Thanks to machine learning, sophisticated algorithmic decision-making processes arguably have become inscrutable, even to their programmers. The emergent gap between what humans and machines know has led some critics, such as Frank Pasquale, to warn against the risks of a *Black Box Society*[32] driven by what Cathy O'Neil dubs *Weapons of Math Destruction*.[33]

At the same time, breakthroughs in artificial intelligence have enabled disenfranchised groups to speak the truth to power by identifying biases and inequities that were previously hidden in

[27] Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES, July 21, 2010, http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.

[28] J. Mitchell Vaterlaus, Kathryn Barnett, Cesia Roche and & Jimmy Young, *"Snapchat is more personal": An Exploratory Study on Snapchat Behaviors and Young Adult Interpersonal Relationships*, 62 COMPUTERS HUM. BEHAV. 594 (2016); *also see* Evan Selinger, Brenda Leong & Bill Fitzgerald, *Schools Fail to Recognize Privacy Consequences of Social Media*, CHRISTIAN SCI. MONITOR, Jan. 20, 2016, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0120/Opinion-Schools-fail-to-recognize-privacy-consequences-of-social-media.

[29] *Why Self-Driving Cars Must Be Programmed to Kill*, MIT TECH. REV., Oct. 22, 2015, https://www.technologyreview.com/s/542626/why-self-driving-cars-must-be-programmed-to-kill/.

[30] Omer Tene & Jules Polonetsky, *Taming the Golem: Challenges of Ethical Algorithmic Decision Making*, 19 N. C. J. L. & TECH. (forthcoming 2019).

[31] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

[32] FRANK PASQUALE, THE BLACK BOX SOCIETY (Harvard University Press, 2015).

[33] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (Crown, 2016).