Data Laws: Regulating the Not-So-Private Private Sector

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Judy Nguyen

May 5, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____

Approved: _____ Date _____
Peter Norton, Department of Engineering and Society

Data Laws: Regulating the Not-So-Private Private Sector

Data protection measures defend individual rights to security and privacy. The framers of the Constitution established a legal basis for privacy in the 4th amendment, which secures a man's home from unreasonable search and seizure (West's, 2008). Developments including the census, postal service, telecommunications, cameras, computers, and internet transformed American lives by implicating their privacy (Solove, 2006). The slow, reactive nature of lawmaking contrasts sharply with Silicon Valley's race to innovate. This conflict, coupled with the private sector's aversion to legal interference, intensifies the tug-of-war between industry self-regulation and government policy. Laws governing online data usage lag behind security breaches, placing consumers at risk as private data stores have long surpassed public records (Strickland & Hunt, 2005). Among social media users, privacy advocates, nonprofits, and foreign regulatory bodies, there is call for Congress to better defend digital rights. Meanwhile, tech companies, data brokers, and advertisers use insidious tactics to prevent any nationwide legal standard governing online information usage. In the U.S., digital privacy and security remain frail as it lacks collaboration between the government, private sector, and international lawmakers.

Review of Research

Brey (2007) contended that "ethical reflection on information technology should not wait until products hit the market, but should be built in from the beginning by making it part of the design process." It is responsibility of the developer to ensure production code upholds secure

privacy measures. Brey warned of breach consequences including economic harm and loss of time, money, and resources. The failure of safety-critical systems could even lead to injury or death. The right to privacy was first defended by the American justices Samuel Warren and Louis Brandeis (1890), who defined privacy as "the right to be let alone." Data management violates this right, first by the posting and aggregation of personal information, and second through the online monitoring of internet users through cookies, profiling or tracking, and spyware (Brey, 2007). According to Langheinrich (2009), the rising internet accessibility presents threats to privacy that can be reduced by employing six principles: "notice, choice and consent, proximity and locality, anonymity and pseudonymity, security, and access and recourse."

Regulation is the key to enforcing data protection principles. Moshell (2004) found that the global market includes nations whose data protection schemes are incompatible with self-regulation. He compared the United States' sectoral approach under which self-regulation is favored to the EU reliance on comprehensive legislation to govern every facet of industry. He asserted that the U.S. relies upon the ability of industry to regulate itself, viewing a "complex legal or regulatory infrastructure as an un undue restriction on the market" despite a global trend toward comprehensive data protection. Although a self-regulatory approach appears less restrictive and more incentive for an adaptable system of protection, it actually leads to data-protection regulation that is decentralized only slightly improved by narrowly legislation targeting designated problem areas. Currently, the U.S. utilizes "a variety of non-exclusive means-industry codes, business organization, and, more recently, third-party programs-of policing themselves and their respective markets" (Moshell, 2004). Wachter and Mittelstadt (2018), recognizing the risk in Big Data analytics and artificial intelligence (AI), presented a case

for more comprehensive laws to combat inference formation from solicited personal data. They claimed that tensions between individual privacy and business interests, or data protection and trade secrets laws are inevitable. Regulation must determine when the right to privacy takes precedence over the private autonomy of decision-makers in order to protect the people.

At the core of data aggregating, ubiquitous computing, Big Data analytics, and AI innovation sit industry giants. Technology companies dominate the private sector and regulate themselves. While some believe self-industry regulation to be stimulating for the economy, others argue that the true price is privacy. Corporations understand the consequences to security breaches in monetary terms, and are incentivized to protect their customer data for fiscal reasons rather than ethical ones. On the surface, the business motives and user's best interests appear to align. However, as innovation increases, as observed by Langheinrich, Wachter, and Mittelstadt, the need for more comprehensive guidelines are required to preserve civil rights. While the literature tends to focus on specific technologies, a handful of entities have come to dominate industries through mastery of the latest and greatest.

Enter the Internet Era

In 1969, the Department of Defense (DoD) contracted Bolt Beranek and Newman Inc. (BBN) to develop "ARPANET," the predecessor of the Internet (Salus, 1998). Leo Beranek, one of BBN's founders, wrote that as the number of connected nodes increased exponentially, ARPANET was superseded by privately supported networks built by IBM and Bell Laboratories (Beranek, 2000). Commercialization of the Internet entailed monitoring to ensure open and fair business. The Internet Society, formed in 1991 by developers of the internet, was created in response to weak oversight by the DoD, rising Internet commerce, and the need for

standardization of internet infrastructure (Leiner et al., 2003). Many third-party organizations formed to compensate for the lack of legislative guidance.

The terrorist attacks of September 11, 2001, led to demands for security, even at a high cost to privacy. The USA PATRIOT Act of 2001 prioritized national security over personal privacy by legalizing a greater level of government surveillance (Solove, 2006). The act redefined online privacy, and expanded “appropriate use” of domestic intelligence gathering, such as wiretapping. Furthermore, the fear of future terrorist attacks prompted lawmakers to pass more invasive measures at the cost of citizens’ privacy. The Electronic Frontier Foundation (EFF), a nonprofit that defends digital civil liberties, reported the 2005 Bush administration coercion of telecommunications carriers to obtain customer call records, unbeknownst to said customers (EFF, 2012). Predictably, people were outraged at the invasion of privacy once news outlets exposed the domestic spying operation. Two *New York Times* correspondents even won a Pulitzer Prize in 2006 for their critical coverage of the National Security Agency’s surveillance (Hornsby & Farmer, 2006). Risen and Lichtblau reported, “the officials say the National Security Agency's interception of a small number of communications between people within the United States was apparently accidental, and was caused by technical glitches at the National Security Agency in determining whether a communication was in fact "international",” and proceeded to disprove these claims (2005). Foreign threats to the country’s safety shifted the power and responsibility to politicians to safeguard its users. The ensuring exploitation of authority was exposed and recognized by the Pulitzer Prize board, who echoed the American people’s concerns that U.S. officials had abused the technology they helped to build.

Privacy and security should not be mutually exclusive. According to Pearson and Benameur (2010), privacy online entails “the protection and appropriate use of the personal

information of customers". Internet security is more established in literature, as an early publication on electronic commerce defines it as safety against a "circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse" (Kalakota & Whinston, 1996). Both security and privacy must be addressed in crafting comprehensive data protection legislation because the loss of personally identifiable information (PII) often leads to the consequences associated with insecure exchanges. This requires coordination between lawmakers and technologists to prevent extreme acts of patriotism at the expense of civil rights.

Tech Giants Triumph in the Electronic Industry Arena

The Federal Trade Commission (FTC) cautions, "if your company makes claims about how you use consumers' information, remember that those promises… must be truthful and supported by appropriate substantiation," in response to Cambridge Analytica's case on illegally harvesting Facebook user data (Fair, 2019). In response to the privacy scandal, Facebook's Mark Zuckerberg said, "I started Facebook, and I'm responsible for what happens on our platform" (Salinas, 2018). Sheryl Sandberg, company COO, apologized in an interview and admitted Facebook's actions "weren't enough, we need to do more to verify and notify" (CNBC, 2018). When asked about government oversight, she insisted "we're not even waiting for regulation" (Romo, 2018). There lies the issue. The leadership owns responsibility for the platform, and have nothing more to compel them to act outside of their own best interests. Sandberg, in saying that they are being proactive and taking measures ahead of legislative action, confirms that presently there is a lack of regulation.

One of TIME Magazine's most influential people in 2018 was Christopher Wylie, the former Cambridge Analytica developer turned whistleblower that exposed Facebook's illicit data sharing. TIME's executive editor noted Wylie's contribution as revealing how "unregulated power is shaping our lives and our world" (Vella, 2018). Wylie's selection as one of the year's most influential individuals is telling of the power held by firms possessing vast amounts of data and the ability to manipulate it. He dismantled Cambridge Analytica, but his insight on the ease in acquiring supposedly secured profiles from 50 million people is indication that data protection measures lack teeth. An interview with Wylie explains his view that, "We have a completely unregulated digital landscape. There is almost no oversight. We are placing blind trust in companies like Facebook to do the honorable and decent thing. ... Even if Cambridge Analytica doesn't exist anymore, what happens when China becomes the next Cambridge Analytica?" (Wylie, 2019). Even before Facebook's involvement with Cambridge Analytica, the FTC Chairman warned in 2011, "Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users. Facebook's innovation does not have to come at the expense of consumer privacy. The FTC action will ensure it will not" (Leibowitz). In the aftermath of Facebook's breach, little can be said about the promises made by the CEO to protect privacy. Meanwhile, a plan to protect market share was successful as Facebook today remains untouched in spite of the FTC's costly settlement.

Often regarded as the leader among tech giants when it comes to privacy, Apple employs an alternative approach to self-regulation. Senior vice president of software engineering at Apple, just before announcing the new Maps features at their Worldwide Developers Conference (WWDC) 2019, assured audience members that "we believe privacy is a fundamental human right and we engineer it into everything we do. This year, we are doing even more" (Federighi,

2019). In terms of iOS feature work, Apple delivered. But a latent function of the update was to appear to lawmakers that they have users' best interests in mind. A proactive approach to securing iPhone data is confirmation that self-regulation works. Except what happens when it does not work? A tech columnist experimented with requesting his personal data from Apple, Google, and Facebook– Google and Facebook's process involved clicking a single button and obtaining a data report immediately. Apple "hides the data request deep inside the privacy section of the website [and] to get there, it's four clicks from the main page and buried in the 11th subhead on the page" (Graham, 2018a). After requesting on Monday morning, the writer received a reply Tuesday morning asking to verify credentials. Eight days later, Graham had the report and the excluded parts were informative than the attachment itself (Graham, 2018b). The report stated that they do not collect individual statistics.

The answer to ensuring privacy is "differential privacy," according to Apple. It is also the reason for Graham's sparse data request. Coined by computer science Professor Aaron Roth, differential privacy allows you "to derive statistical insights from the database as a whole… to prevent some outside observer or attacker from learning anything specific about some [individual] in the data set" (Greenberg, 2016). Roth was referenced in the WWDC 2016, but Apple did little more to state how exactly they would implement differential privacy. While the field of differential privacy expands, as does the accuracy of inferences derived from Big Data analytics and AI. Eventually, the ability to deanonymize data will risk personal privacy. When that happens, there are no sanctions to guarantee that U.S. companies, such as Apple, will be held liable.

When the senior vice president applied technological solutionism to his argument for the effectiveness for industry self-regulation, he undermined Apple's defense in a landmark victory

for encryption security. The Supreme Court set a new precedent in 2016 when it sided with Apple over the Federal Bureau of Investigation (FBI) in a case compelling the tech giant to override an iPhone's security. Apple CEO Tim Cook posted "A Message to Our Customers" describing the case, how encryption works, and what threat this precedent could set if the FBI were successful in cracking the company's security (2016). The justices understood that applying more engineering to crack the encryption would create vulnerabilities in the commonly used security measure. When it best suits their commercial interests, Apple's leadership was swift to point out long-term consequences in the FBI's request. Even though when prompted for explanations about the future of user privacy, Apple is able to invoke the protection of trade secrets.

When Apple revoked Facebook's ability to distribute internal iOS apps after the latter breached the contract by collecting external user data, Cook was applauded for protecting privacy. In reality, he "enforced the terms of a licensing agreement; appearing to fight for user privacy is just a side effect" (Bogost, 2019). And so, the two tech giants, Facebook and Apple, are not too different after all. This is not a crime, as they both behave as any other businesses does in a competitive market. But it calls into question the true efficiency of self-regulating industries at ensuring user rights are protected and enforcing consequences when they are violated.

The Perils of Innovation in the Public Sector

In the healthcare industry, patient data is often sensitive and thus most vital to protect. The Consumer Technology Association (CTA) president and CEO released privacy guidelines on health data, adding they were "developed with consensus among industry stakeholders"

(Shapiro & Cassagnol, 2019). Although these guidelines from are voluntary and vague, this trade organization's attempts to protect patient privacy is the opposite of how the Department of Health and Human Services (HHS) is taking action. The largest electronic health record (EHR) company in the United States, Epic, opposed a rule from the HHS requiring EHRs to become more easily accessible to patients. This was a move to combat expensive and lengthy processes that patients undergo to obtain their own medical records. Hospitals are not incentivized to provide this information as it allows patients to seek care elsewhere. In protest, Epic's CEO, Judith Faulker, sent an email to hospital system leaders urging them to sign a letter indicating disapproval of the HHS proposal (Farr, 2020). On the company's homepage, Epic claimed that the rule presented "serious risks to patient privacy," and explicitly compared the accessibility of a patient to his or her own data to "a situation like Cambridge Analytica" (Epic, 2020). Another facet of privacy involves one of Langheinrich's principles, "choice and consent." Patients should have access to their own data, and Epic's reference to Cambridge Analytica is a scare tactic meant to further their own interest in monopolizing the EHR market. Cerner, Epic's largest competitor, publicly endorsed the HHS's plan in the vice president's blog post saying it "promotes the end of information blocking — a practice in which the access, exchange or use of electronic health information is restricted inappropriately" (Travis, 2019).

Tech giants are beginning to enter the healthcare realm, equipped with resources and funding that public entities lack. Google, having acquired fitness tracker company Fitbit and partnered with Mayo Clinic, sought cloud deals with both Epic and Cerner. However, both EHR companies opted instead for other contracts due to employee "concerns about some of the tools that Google has used to export and import data, which they said aren't fully compliant under HIPAA" (Elias, 2019). Data protection must include specific measures to prevent the wrong

entities from improper access and while enabling authorized users' easy access to their own data. Small pieces of legislation that are too specific, such as the HHS's proposal, tend to be reactive and narrow in scope. There must be balance in short, detailed legislation and broad industry self-regulation in order to apply to any company collecting data.

A D.C.-based nonprofit, the Center for Democracy & Technology (CDT), launched a campaign with goals to pass federal consumer privacy laws and create user-friendly privacy tools to control data sharing. CDT leaders insist, "it's time for privacy law and online practices to catch up with the seismic shifts in technology," and, "restoring the privacy balance in this country won't happen overnight, but it won't happen at all if we don't demand it" (CDT, 2009). Voatz is a mobile voting system founded by Nimit Sawhney. He "understands the need for questions about security, but adds that as a private company he also has to protect his intellectual property" (Abrams, 2019). Voatz would have been the first internet voting application in the U.S., but the Massachusetts Institute of Technology (MIT) published a study revealing vulnerabilities that allow a secret ballot to be recovered and manipulated through a side channel attack (Specter et al., 2020). This conflict between data protection and trade secret rights could have been resolved with proactive regulation that enumerated concrete requirements for Voatz. Incumbent Missouri Senator, Josh Hawley, stated "companies have gotten by with the 'trust us' defense for far too long" (2018).

The Cost of Connectedness

Devices outnumber individuals as industry self-regulation becomes less reliable for preserving civil liberties. Big tech must be held accountable for profitable practices, such as selling user data. Groups such as the American Civil Liberties Union endorse "Civil Rights

Principles for the Era of Big Data" that transfers power from corporations to consumers (Calabrese, 2014). They view privacy as a right that eager businesses infringe upon. More aggressive critics of big tech have formed an anti-social media movement. An ex-Facebooking columnist writes that mainstream social media platforms are "engineered to be addictive… as these companies gather more data about their users, it is becoming more addictive" (Mahdawi, 2018). Individuals like Mahdawi value individual liberties like security and privacy, going so far as to quit social media altogether in order to reclaim control.

Users have little liberty over the content they see. Targeted advertisements are based on age, gender, liked pages, and even browsing history (Berman, 2018). But when such marketing seems intrusive, it can backfire for the advertiser. Users are generally also unaware of the content collected from them. Companies are disincentivized to have user-friendly Terms and Conditions. Instead, the contracts are lengthy and filled with legal jargon– or they are brief but vague to claim maximum allowances (Lomas & Dillet, 2015). Third-party companies are eager to buy this data for profitable use and distribution. Data brokers are businesses that collect and sell personal information. While some let consumers see the data they collect about them, only voluntary guidelines regulate what information is used, and how (Naylor, 2016). These companies build detailed profiles to create a digital identity of everyone online. Data can also be mishandled or leaked to criminals. Smith et al. (2012) found that image meta-data, including GPS coordinates and facial recognition tags, can be compromised. These shield criminals engaged in fraud, theft, and blackmail. Worse still, the threat is not confined to active users. Inactive persons are exposed when family or friends mention them online. Despite these risks, the United States maintains trust in self-regulating industry standards. The Consumer Technology Association has mobilized to represent smaller tech companies, creating a PAC that resists "design mandates that will raise

costs and reduce [the] freedom to innovate" (CTA, 2019). Like tech giants, they object to regulations that impede on profits. However, increasing globalization requires international cooperation in the enforcement of data protection laws.

Although national laws vary, Reidenberg (2000) contends that the world's democracies recognize "information privacy as a critical element of civil society." As more citizens of the world get connected, the amount of data gleaned from online users continues to grow. In 1970, Hessen, Germany was the first adopter of such statutes, when frameworks protecting personal data proved ineffective when the data moves to another jurisdiction (Phillips, 2018). Almost 50 years later, the EU passed General Data Protection Regulation (GDPR) to give users control over their personal data (Marelli & Testa, 2018). The enactment of this binding and enforceable regulation replaced the previous 1995 Data Protection Directive, that was neither as rigorous nor mandatory (Phillips, 2018). The internet has no borders, limiting the effect of national laws. Nonetheless, European Union (EU) laws seek to "protect all EU citizens from privacy and data breaches," and they affect all companies that do business with its residents (EU GDPR, 2019). Despite GDPR being a foreign policy, the United States is still affected since customers include EU constituents.

Conclusion

In response to technological innovation, many third parties formed to provide U.S.-based companies guidance on data protection practices, albeit voluntary and inconsequential. Having examined the debate of security versus privacy, a comprehensive law can and must uphold both to succeed in defending digital rights. Moreover, privacy is not just about denying the wrong people permission– it includes allowing the right people clear access to their own information.

Given that businesses act in their own economic interests, legislators should not trust that corporate leadership will choose civil liberties over intellectual property rights. More technology is not the solution. Yet, the U.S. relies on self-regulation and expects industries to behave ethically without incentive or sanctions. When comparing this economy boosting risk to the extensive EU's regulations, it is crucial to recall that measures such as GDPR reach American markets thanks to increasing globalization. Sooner or later, U.S. enterprises will have to comply. Coordination between international entities, nations, and corporations are the only way to protect everyone online. As modern times become more interconnected, synchronization among these groups will keep sellers accountable to their buyers. Further research into statewide efforts to preserve privacy could demonstrate another case for the United States to pass comprehensive regulation. Demand from foreign heads and governors would indicate a call for action from all directions. Federal lawmakers hold the key to defending internet liberty and justice for all.

References

Abrams, A. (2019, Nov. 3). *Smartphone Voting Could Expand Accessibility, But Election Experts Raise Security Concerns*. Time. time.com/5717479/mobile-voting-accessibility.

Beranek, L. (2000). Roots of the Internet: A Personal History. *Massachusetts Historical Review, 2*, 55–75. JSTOR.

Berman, R. (2018). Beyond the Last Touch: Attribution in Online Advertising. *Marketing Science, 37*(5), 771–792. doi.org/10.1287/mksc.2018.1104.

Bogost, I. (2019, Jan. 31). Apple's Empty Grandstanding About Privacy. *The Atlantic.* www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680.

Brey, P. (2007). Ethical Aspects of Information Security and Privacy. In M. Petković & W. Jonker (Eds.), *Security, Privacy, and Trust in Modern Data Management* (pp. 21–36). Springer. doi.org/10.1007/978-3-540-69861-6_3.

Calabrese, C. (2014, Feb. 27). *When Big Data Becomes a Civil Rights Problem*. American Civil Liberties Union. www.aclu.org/blog/smart-justice/mass-incarceration/when-big-data-becomes-civil-rights-problem.

CDT. (2009, Dec. 3). CDT's 'Take Back Your Privacy' Campaign Will Put Privacy Front and Center. Center for Democracy and Technology. cdt.org/press/cdt%e2%80%99s-%e2%80%98take-back-your-privacy%e2%80%99-campaign-will-put-privacy-front-and-center.

CNBC. (2018, March 23). Facebook COO Sheryl Sandberg: "We Do Not Sell Your Data" [Television]. www.youtube.com/watch?v=p1CTHFEcoJc&feature=youtu.be.

Cook, T. (2016, Feb. 16). A Message to Our Customers. Apple. www.apple.com/customer-letter/

CTA. (2019). Consumer Technology Association Political Action Committee (CTAPAC). CTA. www.cta.tech/Policy/CTAPAC.aspx.

EFF. (2012, Dec. 3). How the NSA's Domestic Spying Program Works. Electronic Frontier Foundation. www.eff.org/nsa-spying/how-it-works.

Elias, C. F., Jennifer. (2019, Nov. 12). Google's Hospital Data-sharing Deal Raises Privacy Fears. CNBC. www.cnbc.com/2019/11/12/google-project-nightingale-hospital-data-deal-raises-privacy-fears.html.

EPIC. (2020, Jan. 27). Electronic Privacy Information Center. Epic Supports Patients' Access to Their Data, Proposes ONC Rule Solutions to Protect Privacy. www.epic.com/epic/page/epic-supports-patient-access-onc.

EU GDPR. (2019). General Data Protection Regulation. eugdpr.org/the-regulation.

Fair, L. (2019, Dec. 6). Commission Issues Opinion in Cambridge Analytica Case. Federal Trade Commission. www.ftc.gov/news-events/blogs/business-blog/2019/12/commission-issues-opinion-cambridge-analytica-case.

Farr, C. (2020, Jan. 23). Epic's CEO is Urging Hospital Customers to Oppose Rules that Would Make it Easier to Share Medical Info. CNBC. www.cnbc.com/2020/01/22/epic-ceo-sends-letter-urging-hospitals-to-oppose-hhs-data-sharing-rule.html.

Federighi, C. (2019, June 4). WWDC 2019 Keynote—Apple. www.youtube.com/channel/UCE_M8A5yxnLfW0KghEeajjw.

Graham, J. (2018a, April 17). Is Apple Really Better About Privacy? *USA Today.* www.usatoday.com/story/tech/talkingtech/2018/04/17/apple-make-simpler-download-your-privacy-data-year/521786002.

Graham, J. (2018b, May 6). Apple Took 8 Days to Give Me the Data it Had Collected on Me. *USA Today.* www.usatoday.com/story/tech/talkingtech/2018/05/04/asked-apple-everything-had-me-heres-what-got/558362002.

Greenberg, A. (2016, June 13). Apple's 'Differential Privacy' Is about Collecting Your Data—But Not Your Data. *Wired*. www.wired.com/2016/06/apples-differential-privacy-collecting-data.

Hawley, J. (2018, May 19). Data Privacy Issues May Be Coming to a Campaign Near You. NBC News. www.nbcnews.com/politics/politics-news/data-privacy-issues-may-be-coming-campaign-near-you-n875461.

Hornsby, R., & Farmer, M. (2006). Pulitzer Prizes 2006. www.pulitzer.org/winners/james-risen-and-eric-lichtblau.

Langheinrich, M. (2009). Privacy in Ubiquitous Computing. In J. Krumm (Ed.), *Ubiquitous Computing Fundamentals* (pp. 95–159). Chapman and Hall/CRC. doi.org/10.1201/9781420093612.ch3.

Leibowitz, J. (2011, Nov. 29). Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises. Federal Trade Commission. www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2003, Dec.). *A brief history of the internet*. dl.acm.org/doi/abs/10.1145/1629607.1629613?casa_token=gQldc4cy8IoAAAAA:N5vWXF3Qzliwljxjo4SfRYrGtaKtaMduPGxbAk16SZkwClXqZqzHEMCJneZVupdLDxOGiGM7YO0zIw.

Lomas, N., & Dillet, R. (2015, Aug. 21). Terms and Conditions Are the Biggest Lie of Our Industry. *TechCrunch*. social.techcrunch.com/2015/08/21/agree-to-disagree.

Mahdawi, A. (2018, Jan. 1). Antisocial media: Why I decided to cut back on Facebook and Instagram. *The Guardian*. www.theguardian.com/lifeandstyle/2018/jan/01/antisocial-media-why-decided-cut-back-facebook-instagram.

Marelli, L., & Testa, G. (2018). Scrutinizing the EU General Data Protection Regulation. *Science*, *360*(6388), 496–498. doi.org/10.1126/science.aar5419.

Moshell, R. (2004). And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend toward Comprehensive Data Protection Comment. *Texas Tech Law Review*, *37*(2), 357–432.

Naylor, B. (2016, July 11). Firms Are Buying, Sharing Your Online Info. What Can You Do About It? NPR. www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it.

Pearson, S., & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 693–702. doi.org/10.1109/CloudCom.2010.66.

Phillips, M. (2018). International Data-sharing Norms. *Human Genetics*, *137*(8), 575–582. doi.org/10.1007/s00439-018-1919-7.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. doi.org/10.1080/17579961.2018.1452176.

Ravi Kalakota, & Whinston, A. B. (1996). *Frontiers of Electronic Commerce*.

Reidenberg, J. R. (2000). Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Review*, *52*(5), 1315–1371. JSTOR. doi.org/10.2307/1229516

Risen, J., & Lichtblau, E. (2005, Dec. 21). Spying Program Snared U.S. Calls. *New York Times*. www.nytimes.com/2005/12/21/politics/spying-program-snared-us-calls.html.

Romo, V. (2018, April 5). Facebook's Sheryl Sandberg on Data Privacy Fail: "We Were Way Too Idealistic." NPR. www.npr.org/sections/thetwo-way/2018/04/05/599770568/facebooks-sheryl-sandberg-on-data-privacy-fail-we-were-way-too-idealistic.

Salinas, S. (2018, March 21). Zuckerberg on Cambridge Analytica: “We have a responsibility to protect your data, and if we can’t then we don’t deserve to serve you.” CNBC. www.cnbc.com/2018/03/21/zuckerberg-statement-on-cambridge-analytica.html.

Salus, P. H. (1998). The Net: A Brief History of Origins. *Jurimetrics*, *38*(4), 671–676. JSTOR.

Shapiro, G., & Cassagnol, D. (2019, Sep. 12). CTA Releases Industry-Developed Privacy Guidelines on Health Data. 26492cf36fb34327bade907622fee7d7.pages.ubembed.com/9716615c-97b6-4cd1-8a93-f86b4b9829c4/a.html.

Smith, M., Szongott, C., Henne, B., & Voigt, G. von. (2012). Big Data Privacy Issues in Public Social Media. *2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST)*, 1–6. doi.org/10.1109/DEST.2012.6227909.

Solove, D. J. (2006). *A Brief History of Information Privacy Law*. 47.

Specter, M. A., Koppel, J., & Weitzner, D. (2020). *The Ballot Is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections*. 20.

Strickland, L. S., & Hunt, L. E. (2005). Technology, security, and individual privacy: New tools, new threats, and new public perceptions. *Journal of the American Society for Information Science and Technology*, *56*(3), 221–234. doi.org/10.1002/asi.20122.

Travis, J. (2019, June 24). Why the ONC Information Blocking Rule Is a Good Sign for the Future of Health Care IT. www.cerner.com/perspectives/why-the-onc-information-blocking-rule-is-a-good-sign-for-the-future-of-health-care-it.

Vella, M. (2018). Christopher Wylie: The World’s 100 Most Influential People. *Time.* time.com/collection/most-influential-people-2018/5238171/christopher-wylie.

Wachter, S., & Mittelstadt, B. (2018). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (SSRN Scholarly Paper ID 3248829). Social Science Research Network. papers.ssrn.com/abstract=3248829.

Waddell, K. (2020, Feb. 11). California Privacy Law Prompts Companies to Shed Consumer Data. *Consumer Reports.* www.consumerreports.org/privacy/california-privacy-law-ccpa-prompts-companies-to-shed-consumer-data.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. JSTOR. doi.org/10.2307/1321160.

West’s Encyclopedia of American Law, edition 2. (2008). *Fourth Amendment*. TheFreeDictionary.Com. legal-dictionary.thefreedictionary.com/Fourth+Amendment.

Wylie, C. (2019, Oct. 8). *Whistleblower Explains How Cambridge Analytica Helped Fuel U.S. "Insurgency."* NPR.Org. www.npr.org/2019/10/08/768216311/whistleblower-explains-how-cambridge-analytica-helped-fuel-u-s-insurgency.