CMI working paper no. 18, 2019

How Policy Is Failing to Secure Privacy on Platforms

Roslyn Layton

Center for Communication, Media and Information technologies (CMI), Electronic Systems, AAU Copenhagen, Denmark

CMI Working Paper no. 18:

Roslyn Layton (2019) *How Policy Is Failing to Secure Privacy on Platforms*

ISBN: 978-87-7152-103-0

Published by:
center for Communication, Media and Information technologies (CMI)
Department of Electronic Systems,
Aalborg University Copenhagen,
A.C. Meyers Vænge 15,
DK-2450 Copenhagen SV
Tel +45 99403661
E-mail cmi@cmi.aau.dk
URL http://www.cmi.aau.dk

How Policy Is Failing to Secure Privacy on Platforms

By Roslyn Layton, PhD
Visiting Fellow, Center for Communication, Media & Information Technologies
Aalborg University, Copenhagen, Denmark
December 2019

Introduction

There is an important policy effort underway in the United States to evaluate consumer privacy legislation for the digital age. The European Union's General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA) are suggested by many as the "gold standard" or "floor" for privacy regulation. Those frameworks would be warranted if in fact the they delivered the expected outcomes. However, as has been shown in the 18 months since the promulgation of the GDPR, the revenues and market shares of the largest internet companies have increased; many small firms have lost market share or have exited the market; and consumer trust online has reached its lowest point in the European Union since 2006. Moreover, the adoption of the GDPR is associated with a number of unintended and negative security consequences including the blocking of public information in the WHOIS internet protocol database, identity theft through the hacking of the Right to Access provision (Article 15) and other provisions, and the proliferation of network equipment with security and privacy vulnerabilities. [1] As this paper describes, the key problem is that policymakers have characterized every online entity as the equivalent of a global platform and imposed regulations meant for the largest players on everyone. Complying with the expensive and onerous rules has thus, unwittingly, become an advantage for the largest companies and has strengthened their market position to the detriment of small and medium sized firms which were promised a "level playing field" as a result of the rules. It is estimated that less than half of all applicable firms comply with the GDPR and many believe they will never be able to comply. Given the size and scale of the platforms, there is a tendency to overdo privacy and data protection regulation when the issues implicated are more correctly addressed with antitrust.[2] A review of the regulatory history, assumptions, and theory is helpful to inform the policy development.

The privacy effort, while overdue, is driven in part by a fundamentalist approach to data in that any personal data in all places and all times is inviolable. This broad and strict interpretation is expressed in the GDPR and the California Consumer Protection Act in which every online entity must purchase a set of software upgrades and implement processes to comply with the government's mandate. The law has been designed with the so-called big tech platforms in mind, notably Microsoft, Amazon, Apple, Alphabet, and Facebook. With a few exceptions, every company with a website, regardless of how small, must fulfill the same obligations. This marks a departure for the US, which hitherto, viewed privacy from a risk-based perspective, imposing obligations only on specific tasks and sectors where harm and its likelihood could be identified, but otherwise allowing the innovative use of personal data with disclosures subject to the Federal Trade Commission's unfair and deceptive standard. The carefully tailored framework in the US consists of literally hundreds of laws on privacy

[1] Layton, Roslyn and Silvia Elaluf-Calderwood. "A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices." IEEE. 978-1-7281-2856-6/19
[2] MacCarthy, Mark, Can Antitrust Enforcement Improve Privacy Protection? Privacy as a Parameter of Competition in Merger Reviews (July 26, 2019). Available at SSRN: https://ssrn.com/abstract=3427317

and data protection including common law torts, criminal laws, evidentiary privileges, federal statues, and state laws which comprise a more than 200 year legal tradition in the protection of individual privacy.[3] The EU's laws are relatively new, officially dating from this century, and still lack the runway of judicial scrutiny and case law that characterizes U.S. law.

Undoubtedly privacy violations by the large platforms have sparked outrage in privacy watchdogs, government officials, and the media. Others, not necessarily outraged, express unease about the business practices of the large platforms on personal data. Rather than focus on the specific firms and violations, the fundamentalist approach of the Californian and European laws has the practical impact of equating every firm, regardless of how to small, to a Silicon Valley behemoth. These new regimes threaten to upend existing hard-fought privacy rules for children and families as well as personal information related to health, finance, telephony, employment, insurance, and so on. The outrage, however justified and legitimate, must be tempered with a rational, evidence-based analysis to the specific firms and violations. It does not seem correct or fair that every firm be equated with the big tech platforms. Few firms enjoy such market power. Microsoft, Amazon, Apple, Alphabet, and Facebook are very different from most online firms for important economic and technical reasons. Ideally policymakers should understand these differences, the distinctions between business models, and which dynamics advantage the platforms.

Big tech platforms are in a class by themselves when it comes to market capitalization, revenue, and users. The market capitalization of Microsoft, Amazon, Apple, Alphabet, and Facebook amount to more than $4 trillion, about one-fifth of the value of the US gross domestic product and a whopping two-thirds of the value of the world's top 30 internet companies.[4] To put this into perspective with the rest of the US economy over a year, the entire construction industry spends about $1.3 trillion; traditional retail $900 billion, and consumer products manufacturing $821 billion.[5] Another telling figure, over 5000 internet service providers in the US generate about $300 billion annually, still smaller than the market capitalization of any one of the internet giants.[6] Given these inequalities, it is confounding why the US has long pursued policies designed to "protect" the big tech players.

This paper will explore these and other important distinctions with the leading platforms and their implications for data privacy and protection. The paper offers a dispassionate review of some of the notable privacy concerns and violations by the platforms, with attention to unfair and deceptive practices, operating systems, virtual assistants, and data sharing with adversarial countries. It also reviews the unintended consequences of these companies' aggressive efforts to enable end to end encryption under the premise of protecting users' privacy. It then describes the leading policy and regulatory responses and their shortcomings. It concludes with a discussion of why European and Californian laws fail to address the problems. The paper introduces the concept of certifiable technical standards for data privacy and protection as an effective alternative. The paper contributes to the policy research field with further discussion of the impact of platforms, comparative analysis of data regulatory regimes, and policy recommendations to update state and federal data privacy rules for the online economy.

---

[3]Daniel J. Solove, *A Brief History of Information Privacy Law* in PROSKAUER ON PRIVACY (2006).

[4]Mary Meeker June 11, 2019 @ Code "Internet Trends 2019," accessed November 21, 2019, https://www.bondcap.com/report/itr19.

[5] Alison Deutch. Investopedia. "The 5 Industries Driving the US Economy." February 14, 2019. https://www.investopedia.com/articles/investing/042915/5-industries-driving-us-economy.asp

[6] Calculated metric based upon publicly available financial statements

Technical features of online platforms

At the basic level, a platform is a set of applications working together as a whole for which a user can access via an account, identification number (ID), profile, or key. The platform will be managed by its owner to achieve a set of business goals while optimizing related priorities whether quality, efficiency, security etc. Such a system can be characterized by it points of control. Just as a linchpin keeps a wheel from sliding off the axel, harnessing a control point is a powerful, efficient way to govern a system. Control points can include user IDs, operating system, payment credentials, and so on. As these platforms grow and gain economies of scale, the more easily they manage control points in the system, adding more capability with seemingly less effort. One need not control the system if one can just manage its control point. A firm's governance of control points, whether they are in the platform's network or not, can strengthen the platform.

Microsoft, Amazon, Apple, Alphabet, and Facebook offer platforms or digital ecosystems with a foundational architectural superstructure on which modules or applications can be added to extend the services. This co-creation among the platform owner, users, and developers tussles between generative innovation and infrastructure control.[7] Some of these generative characteristics include leverage (the extent to which tools make possible a set of activities that would be impossible or prohibitively expensive otherwise), adaptability (the scope of uses tools can be put to and the ease to which they can be modified to extend this range of uses), mastery (ease to adopt tools by a broad audience), accessibility (ease of access to the tools and the information on how to use them), and transferability (degree to which the instrument can be deployed for new uses).[8] Paradoxically what makes the platform so compelling for the user can also give rise to the firm's market power.

Unique Identifiers

The user's ID or key allows her to access the platform (like how keys unlock doors and rooms to a house) and attaches information to that key to optimize the interaction with the platform, a feedback loop. The platforms compete amongst themselves to have the most compelling experiences (or rooms so to speak). In practice, it is not possible to use the key from one platform to access another. This contrasts with mobile networks in which a user can port her mobile number to another carrier and call the same people, a regulated service called number portability. While data portability has been proffered to regulate platforms, data from one platform does not necessarily map to another. For example, one's set of browsed product data in Amazon does plugged into Facebook does not necessarily offer a meaningful experience. It is an understatement to say that these differences will become even more complex as the platforms apply artificial intelligence (AI) and advanced computing techniques to the platform.

The ease of using the platform encourage the user to engage with an increasing number of the platform's apps, products, and services. While this can be recognized as a reflection of the improving quality of user experience, from a privacy perspective, it amounts to an increase in the use of personal information to the system. While being big itself is not a privacy violation, it does increase privacy risk, as breaches and violations can cascade to millions of users almost instantly. Importantly for US information privacy law, the degree of ex ante regulation was informed by the level, degree, and probability of risk.

---

[7] Ben Eaton et al., "Distributed Tuning of Boundary Resources: The Case of Apple's iOS Service System," *MIS Quarterly: Management Information Systems* 39, no. 1 (2015): 217–43.

[8] Ben Eaton, Silvia M. Elaluf-Calderwood, and Carsten Sørensen, "The Role of Control Points in Determining Business Models for Future Mobile Generative Systems," IEEE, 2010.

By way of example, a user may have first used Google by creating a user ID for searches or Gmail in 2004. Over the following 15 years, Google has increased its apps by the hundreds, which the user can access with the same ID. Moreover, that ID effortlessly flows to the Android mobile ecosystem which connects to a world of millions of apps. The privacy transaction of signing up for Google is an order of magnitude far greater than participating in any discrete app the explicit regulation for both is the same. Following is a brief discussion of each of the platforms.

Microsoft

Microsoft is a leading platform company with a market cap of $1 trillion. It operates the Windows software suite, a leading desktop operating system; a leading enterprise productivity tool Office 365 integrated with Skype (the leading provider of long distance calling); Exchange, the enterprise email platform; SharePoint, enterprise resource system; SQL Server, the business intelligence platforms; Xbox, the video game platform; the search engine Bing; Dynamics, ERP and customers relations management software; System Center to manage data centers; Skype, real-time voice and video; and Azure for cloud computing. Microsoft licenses its products to individuals and firms in free and paid versions. The various products collect massive amount of personal data from its interactions between users and its products.[9] Some information users provide directly; in other cases, Microsoft infers it based upon user behavior and interactions. Microsoft also obtains third party data about its users. Microsoft's Enterprise and Development products also use personal data provided by the license owner such as school or business. Microsoft uses the data internally to improve it product develop, marketing, and so on.

The current privacy concerns relating to Microsoft and investigation by the Ireland's Data Protection Commission involve both the installation and ongoing use of Windows 10, with focus on the non-diagnostic data that Microsoft collects. There are various requests for data collection that are made during the Windows 10 installation and setup processes. The data authority wants to know if the user consent to this data collection is appropriately informed or not, along with the question of whether Microsoft is collecting more data than is necessary.

Amazon

Amazon, $888 Billion market cap, bills itself as the "Earth's most customer-centric company, where customers can find and discover anything they might want to buy online, and endeavors to offer its customers the lowest possible prices." It has some three dozen different business lines including its flagship retail operation with a specialty in consumer electronics and white label products; Prime, its subscription service including its own delivery fleet of vans; digital content including games, books, music, movies, on-demand video; online marketplace for art; cloud computing platform; cloud storage; movie studio for original films; book publishing; enterprise IT services (Amazon Web Services); philanthropic giving platform; food, produce, and home delivery (built on its acquisition of Whole Foods), Amazon Wireless (mobile network virtual operator); event tickets platform; home repair service platform connecting workers with Amazon customers; restaurant reservations platform; payment processing, the WorkMail email/scheduling service; branded semiconductors, the Alexa home assistant, an online application store, and so on. Amazon CloudFront is a content

[9] "Microsoft Privacy Statement – Microsoft Privacy," June 2019, https://privacy.microsoft.com/en-us/privacystatement.

delivery network that delivers data, videos, applications, and APIs with low latency and high transfer speeds,[10] With CloudFront it is possible to enforce end-to-end HTTPS.[11]

Amazon is well-known for its big data capabilities, but while it has massive amounts of data, it fine tunes its product recommendations to individuals to not overwhelm them with information. It uses a process called "collaborative filtering", deciding what it thinks the customers wants by building up a picture, and then offering products that people with similar profiles have purchased. As Bernard Marr explains, "This mountain of data is used to build up a "360-degree view" of you as an individual customer. Amazon can then find other people who fit into the same precise customer niche (employed males between 18 and 45, living in a rented house with an income of over $30,000 who enjoy foreign films, for example) and make recommendations based on what those other customers like."[12]Amazon collects many kinds of personal information,[13] notably that which the customer providers by entering it into the website. Its cookies collect the information that user create as the access different Amazon services. Amazon collects a suite of mobile information from the its mobile apps. It maintains an email program with analytics to track to steward the retail process, and it studies its customers by purchasing information from third parties to see their footprint and preferences on other platforms. preference to those from data brokers to ensure that it does not send too many emails. Amazon also uses personal information to cross market its products and services to its customers.

Concerns have been raised about the extent of Amazon's customer profiling, its use of attributes-based processing to find similar customers, and issues with browsing and cookies. Separately, Amazon was able to incubate with a unique set of factors such as the investors who were comfortable with losses while it gained market share and profitability; the dearth of sales tax; brick-and-mortar competitors that shouldered many labor, environmental, and other regulations it did not; and regulatory decisions that deterred retailers from mergers that would have otherwise increased its competition. Amazon's control points include digital book pricing, an area in which it attempted to be price maker, but a challenge from publishers has changed how prices are negotiated.[14] As a platform for third parties, Amazon faces conflicts over contract terms, alleged cannibalization with white label products, and proliferation of banned, unsafe, and mislabeled products.[15] Similar concerns have been raised around Amazon Web Services (AWS), for example that it mines the data of retailers for insights to improve its own ecommerce.[16]

---

[10] "Content Delivery Network (CDN) | Low Latency, High Transfer Speeds, Video Streaming | Amazon CloudFront," Amazon Web Services, Inc., accessed July 12, 2019, https://aws.amazon.com/cloudfront/.
[11] "Secure Your Content Delivery Network with Amazon CloudFront," Amazon Web Services, Inc., accessed July 12, 2019, https://aws.amazon.com/cloudfront/security/.
[12] "Amazon: Using Big Data to Understand Customers," Bernard Marr, accessed July 12, 2019, https://www.bernardmarr.com/default.asp?contentID=712.
[13] "Amazon Privacy Notice," Amazon, August 29, 2017, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496.
[14] Amazon, "Apple eBooks Antitrust Settlement," https://www.amazon.com/gp/feature.html?ie=UTF8&docId=1002402851.
[15] Alexandra Berzon, Shane Shifflett, and Justin Scheck, "Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products," *Wall Street Journal*, August 23, 2019, https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990.
[16] See Jay Greene and Laura Stevens, "Wal-Mart to Vendors: Get Off Amazon's Cloud," *Wall Street Journal*, June 21, 2017, sec. Tech, https://www.wsj.com/articles/wal-mart-to-vendors-get-off-amazons-cloud-1498037402. https://www.cnbc.com/2017/06/21/wal-mart-is-reportedly-telling-its-tech-vendors-to-leave-amazons-cloud.html. Christina Farr Levy Ari, "Target Is Plotting a Big Move Away from AWS as Amazon Takes

Apple

Apple Inc., market cap $875 billion, is known for its signature products the iPhone smartphone, the iPad tablet computer, the Mac personal computer, the iPod portable media player, the Apple Watch smartwatch; the Apple TV digital media player and so on. Its services include iTunes, the Safari web browser, iLife and iWork productivity suites, It provides operating systems for its various devices and professional applications for video/filmmaking, music/audio, and software development. Its online services include the iTunes Store, the iOS App Store, Mac App Store, Apple Music, Apple TV+, iMessage, and iCloud. Other services include a suite of financial products services such as Apple Pay, Apple Pay Cash, and Apple Card.

Apples uses personal information, frequently in collaboration with third party information, to improve its products, services, content, and advertising; for loss prevention and anti-fraud purposes; and pre-screening or scanning uploaded content for potentially illegal content.[17] Apple notes that in addition to standard information such as name, mailing address, phone number, email address, contact preferences, it also collects device identifiers, IP address, location information, credit card information and profile information from social media. Apple also collects the information its customers shares when they send gift certificates and products to others or invite others to participate in Apple services. Apple uses the information to market it news products and services to existing customers, notably by using age to market certain services. For certain online transactions, Apple may verify personal information with publicly accessible sources. Apple notes, "For research and development purposes, we may use datasets such as those that contain images, voices or other data that could be associated with an identifiable person. When acquiring such datasets, we do so in accordance with applicable law in the jurisdiction in which the dataset is hosted. When using such datasets for research Apple also notes that it collects information which is not necessarily linked to an individual such as occupation, language, zip code, area code, unique device identifier, referrer URL, location, and time zone to better understand customer behavior and improve products, services, and advertising. Apple also studies user behavior on this many properties and platforms, how customers use services, devices, and apps, including search queries.

In addition to standard cookie information, Apple studies Internet Protocol (IP) addresses, browser type and language, Internet service provider (ISP), referring and exit websites and applications, operating system, date/time stamp, and clickstream data. Apple note that to provide location-based services that it may collect and/or share precise location data, GPS, Bluetooth, IP Address, crowd-sourced Wi-Fi hotspot and cell tower locations, and other technologies.

Privacy concerns have been raised about how Apple works with third parties by pulling data from other platforms to get a better picture of customers, how it studies its customers' web browsing, and its virtual assistant Siri.

Alphabet

Alphabet Inc., market cap $741 billion, is the multinational conglomerate containing Google and its subsidiaries. Google is the single most visited website in the world, and its flagships products are the leaders globally including Search, YouTube, Maps, Android operating system, Chrome web browser

---

over Retail," CNBC, August 29, 2017, https://www.cnbc.com/2017/08/29/target-is-moving-away-from-aws-after-amazon-bought-whole-foods.html. Samantha Ann Schwartz, "Dramatic or Justified? Retailers' Fears Push Cloud Customers from AWS to Microsoft, Google," CIO Dive, November 30, 2018, https://www.ciodive.com/news/dramatic-or-justified-retailers-fears-push-cloud-customers-from-aws-to-mi/543273/.

[17] "Apple Privacy Policy," Apple Legal, May 9, 2019, https://www.apple.com/legal/privacy/en-ww/.

and Chrome operating system. It's Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

It also operates business lines using personal information including online advertising, search engines, cloud computing, software, and internet access with businesses such as Google Fiber, Google Fi, and Google Station. Among its 200 apps include Blogger, Docs, Sheets, Slides and Gmail, Calendar, Drive for cloud storage; Translate, and Photos. It also has some popular devices such as the Home smart speaker, the Wi-Fi mesh wireless router and the Daydream virtual reality headset.

On Google's privacy page it includes 30 versions of its earlier privacy policy going back to 1999.[18] The latest update is a crisp 29 pages and disclosed tidbits such as Google saves names of people to whom the one emails most frequently to provide the autofill feature. It describes the many applications of its unique identifiers include security, fraud detection, email syncing, preferences such as language, and personalized advertising. Unique IDs are also used to recognize a specific device or app and deliver personalization.

In addition, the personal information that the user provides such as name, password, phone number, and payment information, Google also collects the content the user creates, uploads, or receives such as email, photos, videos, and documents. Google also collects information about the user's apps, browsers, and devices.

Other information Google may collect include search terms, watched videos, ad engagement, spoken information to audio apps, purchases, people with whom the user engages, activity with third party sites, and browsing history. For those users accessing the call and messaging apps Google Hangout, Voice, and Fi, Google will collect telephony information such as call logs, dialed numbers, receiving numbers, forwarded numbers, call type, routing information, and time, date, and length of calls. Google collects significant location information with mobile devices including GPS, IP address, device sensor data, and Wi-Fi access points, cell towers, and Bluetooth-enabled devices near the device.

Google also matches and displays publicly available information about the user to its search engine, for example an article about the user that appears in the newspaper. Google also collects information about the user from third party marketing and security partners.

Google describes that it collects the data build better services, to improve the quality of its searches, and to make its ads more compelling. It claims that ads cannot be based on the user's race, religion, or sexual orientation and that it does not provide user's name or email to third party unless the user gives permission.

Some of Google's privacy violations are detailed in the next section.

Facebook

Facebook is an online social network platform with a suite of services, tools, and products for users to engage with each other by posting stories, pictures, and videos. It owns and operates the world's largest messaging services Messenger and WhatsApp; Instagram; the smart AI camera Portal, and virtual reality platform Oculus. Facebook offers a set of tools for application developers to create apps on the platform. If offers a range of marketing services for advertises. Facebook offers a set of tools for workplace productivity, non-profit organizations and educators, small and medium sized organizations, AR/VR creators, and journalists/media. Facebook also runs the Calibra currency and

[18] "Google Privacy Policy," Google, January 22, 2019, https://policies.google.com/privacy?hl=en.

commerce platform. Facebook key platform components include the application program interface for Facebook, the social plugins which allow Like Buttons to appear on other sites across the web, the Open Graph protocol which allows developers to integrate websites into Facebook, authentication protocols which help users connect and share on and off Facebook.

Facebook offers a "Data Policy"[19] probably because the term privacy means so many different things in the many countries it operates. Facebook describes that it collects the information, content, and communication that users provide including metadata such as location and date. Facebook collects information about the people, pages, accounts hashtags, and groups with whom its users engage. It also collects contact information, address books, call/message logs. It collects information about how its products are used, transactions made with them, and interactions with others. Facebook also collects information about the devices integrated with Facebook such as computers, phones, Smart TVS, and other devices including device attributes, its operation, identifiers, signal, settings, network connections, and cookie data. Facebook also collects facial recognition data. This information from across a range of points is used to create personalized advertising. Additional location information collected includes where the user's current location, where one lives, places one likes to go, businesses and people to whom one's near, GPS, IP address, and other information (e.g. check-ins, events).

Facebook collects information from its partners such as advertisers, app developers, and publishers, notably the users' activity off Facebook. Facebook claims that it uses this information to "provide, personalize, and improve" its products.

Privacy Violations and Concerns

Unfair and Deceptive Practices

In the US context privacy violations emerge around deception, fraud, lack of disclosure, and breach of contract. For example, a firm collects data when it doesn't. Alternatively, a firm may say that the information is used one set of purposes under a set of conditions (security), but then is used for another, likely conflicting, purpose for which the user has not given permission (advertising). Alternatively, the firm may purposely obfuscate or deceive the user about the extent to which it uses the information and which information it collects. A related problem is the lack of disclosure about how information is used. Severity of the violation can have to do with the data exposed, the length of time the violation is ongoing, the number of users involved, and the intent of the firm. The law also distinguishes between mere negligence, such as personal information violated by accident versus willful disregard of the law.

The main federal privacy law in the U.S. is 15 U.S.C. § 45, which charges the Federal Trade Commission (FTC) with preventing "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[20] In matters of privacy, the FTC's role is to enforce privacy promises made in the marketplace by suing companies that make such promises and then break them. Whereas the GDPR assumes that any data collection is suspect and therefore regulates it ex ante, the FTC focuses its enforcement efforts on sensitive information that should be protected against unwarranted disclosure. This helps avoid imposing costly and draconian compliance mandates on entities which are not a priori threats to personal privacy, such as personal blogs, small businesses, and informational websites. The FTC's approach seeks to allocate scarce regulatory resources to prevent the greatest threats to online privacy. To be sure, if a small entity behaves in an unfair or deceptive way, it can be prosecuted, but the FTC does not assume that every

[19] Facebook. Data Policy. Accessed November 22, 2019. https://www.facebook.com/policy.php
[20] 15 U.S.C. § 45 (2012).

entity wants to harm online users. Several additional laws form the foundation on which the FTC carries out its charge: the Privacy Act of 1974,[21] the Gramm-Leach-Bliley Act,[22] the Fair Credit Reporting Act,[23] and the Children's Online Privacy Protection Act.[24]

It should be noted that the US was the first country to adopt an information privacy law, the 1974 Privacy Act and since then has adopted some two dozen federal privacy laws based upon the known risks.[25] What has allowed the Privacy Act to endure is not the notion of privacy as a fundamental right of individual control (an idea it rejects), but rather the *mutual interest* of the individual and the data collector to maintain the accuracy and reliability of the personal information. Moreover, the US has extensive laws regulating the government's handling of personal information, dating since the 1700s.[26] The US has not only frequently and significantly updated its privacy laws, it has the longest legal tradition for protecting personal privacy.

The FTC can enact tougher standards on certain firms by entering into consent decrees, agreements made between the FTC and a covered firm, frequently without admission of guilt or liability. Consent decrees frequently include settlements in which a firm will pay a fine and promise to adhere to a specific set of practices. Such instruments are created to create a regime in which the FTC can provide oversight to the company without legal retaliation by the firm.

As the following cases will show, FTC consent decrees have become significantly more stringent, calling for comprehensive information security programs designed to protect the security, confidentiality, and integrity of their users' personal information. For example the firm must describe the content, implementation and maintenance of the privacy program; designate a qualified employee to be responsible for the program; evaluate the effectiveness of the program at least once a year or promptly in the event of a breach; incorporate into the program safeguards appropriate to the risk of harm to users; assess the effectiveness of the safeguards at least once a year or promptly in the event of a breach; and insure that any outside contractors handling its users' information have in place equivalent safeguards. The companies agreed to have the effectiveness of their security programs assessed at every two years for 20 years by a qualified, objective, independent third-party "assessor" who must have a professional qualification such as Certified Information System Security Professional, Certified Information Systems Auditor or the equivalent. The companies also committed not to make any misrepresentations to their assessors. In addition, someone in a senior management position in each company with personal knowledge of their

[21] 5 U.S.C. § 552a.
[22] 15 U.S.C. §§ 6801-6809.
[23] 15 U.S.C. § 1681 et seq.
[24] 15 U.S.C. §§ 6501-6506.
[25] This includes Family Educational Rights and Privacy Act of 1974, the Right to Financial Privacy Act of 1978, the Video Privacy Protection Act of 1988, the Telephone Consumer Protection Act of 1991, the Driver's Privacy Protection Act of 1994, the Health Insurance Portability and Accountability Act of 1996, the Children's Online Privacy Protection Act of 1998, and the Gramm-Leach-Bliley Act of 1999.Other examples of risk-based information privacy laws are the Privacy Act, ERISA; the National Labor Relations Act; the Internal Revenue Act; the Bank Secrecy Act; HIPAA; the Family and Medical Leave Act; the Genetic Information Nondiscrimination Act; the 21st Century Cures Act; the Occupational Safety and Health Act; the Telemarketing and Consumer Fraud and Abuse Prevention Act; CAN-SPAM Act; Electronic Communications Privacy Act (including the Wiretap Act, Stored Communications Act and Pen Register Act; the Cybersecurity Information Sharing Act; and the Whistleblower Protection Act.
[26] See Daniel J. Solove, "A Brief History of Information Privacy Law," in *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, ed. Kristen J. Mathews (New York, Practising Law Institute, 2006).

security programs' operations must file a certification with the FTC annually confirming their continued compliance with the consent orders.

Google and YouTube, September 2019

The FTC and New York Attorney General claim that YouTube violated the Children's Online Privacy Protection Act (COPPA) Rule by collecting personal information ostensibly from children who viewed child-directed channels via a persistent identifier or cookies that tracks users across the Internet, without first notifying parents and getting their consent.[27] The COPPA rule requires that child-directed online services and third party advertisers provide notice and consent of parents prior to information collection for children under the age of 13. From the complaint, it appears that Google deceptively marketed the child version of YouTube to advertisers and toy companies while downplaying if not dismissing the COPPA requirements. The advertisers subsequently created "channels" on the platform with enabled behavioral advertising tools. The complaint further claims that YouTube earned millions of dollars from this illicit activity. The FTC fined Google and YouTube $170 million, of which $136 million goes to the FTC and $34 million to New York. In total, the fine is the largest ever paid for a COPPA violation. This amount is three times larger than the French data protection authority proposes for a transparency and consent violation of the GDPR, seven times larger than the fine imposed by the FTC in 2012 related to its Buzz social network, and 24 times larger than the fine imposed for Google's cookies in the Apple Safari web browser. The FTC also requires that Google and YouTube inform their advertisers of the COPPA requirement and implement a system for channel owners to identify the child directed content and ensure COPPA compliance.

Facebook, July 2019

According to the FTC, Facebook subverted users' privacy choices to serve its own business interests.[28] By 2010, Facebook's default settings for third party apps collected not only the primary user's information, but that of the user's friends. Unwittingly users were subjected to app information collection without their knowledge or permission. Facebook was censured by FTC and entered into a consent decree to halt the practice, and the FTC required users to enable feature such that users could select their privacy settings (whether or not the app would collect data), but Facebook continued the practice for some time with at least tens of millions opting for privacy settings which were not honored. Facebook also failed to maintain a reasonable privacy program that safeguarded the privacy, confidentiality, and integrity of user information. Moreover, it did not vet third party developers. Facebook also asked users for information for security purposes which was used for advertising, violating the FTC Act. In April 2018 when communication with users about its facial-recognition technology, Facebook implied that users had to opt-in for it to work, but Facebook automatically upgraded users to the technology without their consent. Users had to opt out in order not to be subjected to facial recognition. While Facebook was checked by FTC every two years, it did not reveal the illegal practices nor were they found by the FTC.

To address these violations, the FTC imposed a record-breaking $5 billion penalty and extensive conduct relief. The penalty represents 9 percent of Facebook's 2018 revenue, and approximately 23% of its 2018 profit. It is 20 times greater than GDPR fine under similar circumstances. The FTC believes that the magnitude of the fine resets the baseline for privacy cases and sends a strong

[27] "Google LLC and YouTube, LLC," Federal Trade Commission, September 3, 2019, https://www.ftc.gov/enforcement/cases-proceedings/172-3083/google-llc-youtube-llc.
[28] Facebook. Federal Trade Commission, July 24, 2019, https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc

message to firms in future. In addition to substantive privacy and data security requirements, Facebook must implement significant structural reforms to ensure greater corporate accountability, more rigorous compliance monitoring, and increased transparency. This includes greater oversight required of developers; controls on biometric information (the first FTC order to do so); a new corporate governance structure with a specific board of directors for privacy; monitoring by an independent 3rd party and the FTC; and a stipulation that CEO Mark Zuckerberg is personally responsible for compliance/review certifying quarterly under threat of civil and criminal penalties. The investigation and settlement were concluded within a year under existing law by existing resources at FTC.

Microsoft, August 2002

The FTC claimed the Microsoft did not maintain a sufficient level of security to protect the privacy of customers of its Passport and Passport Wallet services, including not implementing and documenting procedures, failure to detect unauthorized access, insufficient monitoring of vulnerabilities, and insufficient recordkeeping on its security and privacy program.[29] The Passport services allowed customers to collect and store credit card numbers and billing/shipping addresses to be used for making purchases across the web. The FTC further alleged the Microsoft was false and misleading in how it represented the program to customers. The FTC entered a consent decree with Microsoft requiring them to implement an information security program with fines for any subsequent violations under the program. Today Microsoft's Passport program has been subsumed into the larger security architecture of Windows 10, specifically the Windows Hello application which uses a PIN or biometrics identifier with encrypted keys from a user's device to provide two-factor authentication.

Operating Systems

Microsoft Windows is the most used operating system for desk top computers, and Google Android for mobile devices. Apple iOS, another leading operating system, runs all Apple devices. The operating system (OS) is the software that supports a computer's basic functions. The OS manages memory and processes and runs its software and hardware. The OS also facilitates user interaction with the device. Originally operating systems were operation manuals, like the booklet provided in the glove box of a car explaining the features of the car. Developers use operating systems to access baseline data about the workings of an application. This information is frequently called telemetry: data to monitor performance remotely, especially crashes and errors. Finding and improving deficiencies help improve the system through patches, updates, and successive versions. Today however operating systems are far more sophisticated, governing the platform ecosystem and tracking user behavior for marketing purposes. Transforming the operating system from a mere analytics dashboard to a commercial marketing system is part and parcel of the realization of modern smartphones.

While users may agree to a specific application or task, that app interacts within a larger operating system where other data collecting and processing apps reside. It is not just the behavior of the app itself which can be observed but is interaction within and across the operating system. A platform owner can learn much more about the user as she moves across the operating system, that a mere provider of a single app.

[29] "Microsoft Corporation, In the Matter Of," Federal Trade Commission, August 8, 2002, https://www.ftc.gov/enforcement/cases-proceedings/012-3240/microsoft-corporation-matter.

Google Android

The operating system serves as the central software part of a device containing the information of the system, all the inputs and outputs of the device, notably the log of calls and messages and the bank of photos, videos, contacts, and calendar. Android records the users' keystrokes, words, and viewed images. Android sees the information a user types before it is encrypted. Android sees the decrypted message once it's received. Android sees all browsing data, the URLs entered, search terms, pages visited and specific clicked items, logins, time spent on content, file uploads and downloads, IP address, bookmarks, app user history, and more. It has location history such as the device location, coordinated with cell tower information, Wi-Fi, and Bluetooth.

Android's capabilities extend to data collected by sensors, webcams, microphones, and any other mobile attachments. In the earlier versions, app developers were able to access, profile, and track "persistent" identifiers such as the Android ID, International Mobile Equipment Identity number,[30] hardware addresses, and SIM serial card number.[31] The advertising ID is the user's digital marketing fingerprint that is consistent across the apps and devices they use. With the "advertising ID" asset, Android can work more closely with app developers and advertisers to provide more relevant advertising to the user and monetize the experience. Android assigns unique and global advertising identifiers, more comprehensive than cookies, to devices and allows apps to access that unique identifier for each device running the operating system.[32] These data are collected and processed from users, both to make the systems and applications work better and to provide insights to advertisers. Data from the operating system may be combined with personal data from other systems for marketing, research and development, and so on. For these reasons, the Android operating system can be provided to the end user without an out-of-pocket cost[33].

Android's capabilities extend to data collected by sensors, webcams, microphones, and any other mobile attachments. In the earlier versions, app developers were able to access, profile, and track "persistent" identifiers such as the Android ID, IMEI number,[34] hardware MAC address, and SIM serial card number.[35] The advertising ID is users' digital marketing fingerprint that is consistent across the apps and devices they use. With the "advertising ID" asset, Android can work more closely with app developers and advertisers to provide more relevant advertising to the user and monetize the experience. Android assigns unique and global advertising identifiers, more comprehensive than cookies, to devices and allows apps to access that unique identifier for each device running the

[30] The International Mobile Equipment Identity is a number, usually unique, to identify 3GPP and iDEN mobile phones and some satellite phones.
[31] John E. Dunn, "Thousands of Android Apps Bypass Advertising ID to Track Users," Sophos, February 19, 2019, https://nakedsecurity.sophos.com/2019/02/19/thousands-of-android-apps-bypass-advertising-id-to-track-users/.
[32] Android Software Development Kit, "Android Software Development Kit License Agreement," Android, http://developer.android.com/sdk/terms.html; Tune Help, "Google's Advertising Identifier," February 21, 2014, https://help.tune.com/marketing-console/googles-advertising-identifier/; and Apple SDK agreement.
[33] Jacob Kastrenakes, "Google Will Start Charging Android Device Makers a Fee for Using Its Apps in Europe," The Verge, October 16, 2018, https://www.theverge.com/2018/10/16/17984074/google-eu-android-licensing-bundle-chrome-search.
[34] The International Mobile Equipment Identity or IMEI is a number, usually unique, to identify 3GPP and iDEN mobile phones, as well as some satellite phones.
[35] John E. Dunn, "Thousands of Android Apps Bypass Advertising ID to Track Users," Sophos, February 19, 2019, https://nakedsecurity.sophos.com/2019/02/19/thousands-of-android-apps-bypass-advertising-id-to-track-users/.

operating system.[36] These data are collected and processed from users, both to make the app work and provide the service at little to no cost because it is subsidized by advertisers. Google, advertisers, and developers may be combined with personal data collected from apps for research and development.

The introduction of Android's Advertising ID in 2013 was billed as privacy-friendly because the user now had capability to reset the ID. However, some apps still reached the user through persistent categories of identification, apparently in violation of Google's policies.[37] Google has just released the 10th version of Android, "Q," in which it promised an improved user interface for privacy settings and stricter permissions and restrictions on what data apps can use.[38]

It appears that Google may push the envelope of its capabilities in its product development, only to find that it oversteps, whether intentionally or not, in the personal information it collects, processes, and shares. While it is laudable that subsequent versions attempt to improve and refine the operating system to make it more private, [39] the fact remains that Google—and its partners—continue to use personal data collected from billions of Android devices and users over years, data that it now realizes should be treated more carefully. It does not appear that Google expunges the data that it collected before, for example, though theoretically users could request this.

Aside from the seeming creepiness, there are some practical uses for such granular detail, notably with location-based services such as Google Maps. The program is so useful that it has made paper maps all but obsolete. However, Google Maps requires heavy-duty data processing to be relevant. Indeed, Google's Mobile Network Insights service, a map showing carriers signal strengths and connection speeds, was so accurate that ISPs accessed it to improve weak spots in their network. However, Google recently shuttered the program due to privacy concerns.[40] A similar program, Facebook's Actionable Insights, is still ongoing.

On a related note, a recent court ruling in Denmark found that the use of mobile location data used in prosecution for thousands of court cases has been deemed inaccurate and imprecise, resulting in the nullification and acquittal of hundreds of people convicted. Some 10,000 cases must be retried as a result. The Danish ISPs explained that their network systems are built for managing the network, not to conduct marketing or surveillance.[41] Hence, the Danish Minister of Justice concluded that attempt to use network information for prosecution is an ill-fitted application.

---

[36] Android Software Development Kit ("SDK"), "Android Software Development Kit License Agreement," Android, (http://developer.android.com/sdk/terms.html)6 "Google's Advertising Identifier," Tune Help, Feb. 21, 2014, (https://help.tune.com/marketing-console/googles-advertising-identifier/).7 Apple SDK agreement.
[37] Serge Egelman, "Ad IDs Behaving Badly – The AppCensus Blog," accessed November 21, 2019, https://blog.appcensus.io/2019/02/14/ad-ids-behaving-badly/.
[38] "Privacy in Android 10," Android Developers, accessed November 21, 2019, https://developer.android.com/about/versions/10/privacy.
[39] Ron Amadeo, "Android 10—The Ars Technica Review," Ars Technica, May 9, 2019, https://arstechnica.com/gadgets/2019/09/android-10-the-ars-technica-review/.
[40] "Exclusive: Fearing Data Privacy Issues, Google Cuts Some Android Phone Data for Wireless Carriers," *Reuters*, August 20, 2019, https://www.reuters.com/article/us-alphabet-data-exclusive-idUSKCN1V90SQ.
[41] Letter from the Minister of Justice: http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2019/brev_til_reu_1.pdf Letter from Danish Attorney General: http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2019/bilag_0.pdf http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2019/justitsministeren-nedsaetter-den-uafhaengige-kontrol-og

Separately, Android has been the focus of antitrust investigations abroad related to the bundling of the operating system with Google's suite of applications, the legality of derivative versions of the operating system, and alleged exclusionary licensing of its operating system. The efficacy of these approaches in promoting innovation and alternatives remains to be seen, and there are some questions as to whether the EU properly applied competition law.[42]

Microsoft Windows

What is called Microsoft Windows is group of various operating systems joined together and sold by Microsoft, usually with a software license. It included components such as Calculator, Calendar, Cardfile, Clipboard view, Clock, Control Panel, Notepad, Paint, Write, and so on. Launched formally in 1985 as an operating system for personal computers, Windows has become the dominant operating system for standalone computers and laptops with more than 90 percent market share.

Presently Windows 10 is under investigation by Ireland's Data Protection Authority. In 2016 French DPA ordered Microsoft to stop tracking Windows 10 users, as it sent telemetry data, including location, text input, touch input, and sites visited to Microsoft.

Apple iOS

Operating systems are the subject of considerable conflict. The Apple iOS platform ecosystem offers a rich field for research with millions of devices, over half a billion users, and millions of apps. An information systems analysis examined 4,664 technical articles published from 2007 to 2011 on the topic of contested innovation on the iOS operating system.[43] Some 30 incidents were cited as disputes between Apple and other actors over "boundary resources," the interface between the platform and developer. These incidents emerged over time, and many are ongoing today and reflect the general nature of the rivalry over sharing resources, notably Apple's rules about the language in which third-party apps must be written, how to migrate its customer base to new devices and systems, and even controversial judgments about whether some apps are politically unacceptable.

Intelligent Virtual Assistants (IVA)

An intelligent virtual assistant (IVA) or intelligent personal assistant (IPA) is a software application that performs tasks or services for an individual based on commands or questions. The assistants use artificial intelligence to perform as robots, speaking in languages and tones that mimic human speech and well as performing tasks that humans can do such as turning on the light or setting the alarm clock. The branded versions are Amazon's Alexa and Echo, Google's Home and its general voice assistant, Apple's Siri, and Microsoft's Cortana. For privacy, the user agrees to terms of use and privacy disclosure. However, privacy in practice with these computers is complex because the assistants become "nurturing" causing the human to forget the assistant is a machine and to forget that it's recording one's private conversation.

For example, Amazon is now being investigated for its Alexa device recording audio from children without first getting consent from their parents, violating the COPPA rule.[44] A class action lawsuit has

---

http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2019/a_-_bilag_1_til_brev_til_reu_-_kommissorium_for_den_uafhaengige_kontrol-_og_styregruppe.pdf

[42] Bergqvist, Christian and Rubin, Jonathan, Google and the Trans-Atlantic Antitrust Abyss (March 18, 2019). University of Copenhagen Faculty of Law Research Paper No. 2019-73. Available at SSRN: https://ssrn.com/abstract=3354766

[43] Supra Eaton 2015

[44] Submission by Campaign for a Commercial Free Childhood to Federal Trade Commission on Amazon Echo Dot Kids, February 9, 2019. https://www.echokidsprivacy.com/#readcomplaint

been filed against Apple lack of disclosure that Siri recorded users' audio.[45] Google is also coming under scrutiny for recording conversations.[46]

Sharing Data with Adversarial Governments

In an illicit effort to get access to sensitive data, some countries require that the platforms store the data within their geographic borders. This is a standard operating practice in China, one so invasive that Facebook closed its operations there and left the country. However, Apple and Google decided to partner with the Chinese government.

University of Virginia China internet policy expert Aynne Kokas describes how China influences standard-setting through national regulation, industrial dominance, and multi-stakeholder organization.[47] Notably Chinese law requires many IT firms to insources data to China, storing it on government-run servers. Meanwhile China exports its laws through the practices deployed by Chinese companies abroad. A type of "cybersovereignty",[48] China's policy is an extension of asserted territorial rights, like those to the South China Sea and Taiwan Straits, to the digital domain. Kokas says a change in the status quo from the last 30 years is needed, for it the Chinese continue, their regulatory framework will transform the ownership and circulation of the data of US companies. Corporate terms of service can drive outcomes in industrial bodies as well as multi-stakeholder organizations.

Kokas observes, "US firms operating in China have repeatedly demonstrated a willingness to leverage the soft power emerging from their brands in the service of Chinese national interests, provided there is a business case for doing so…Apple leveraged access to data that can contribute to the dominance in the future-changing technology of AI." Apple stores the data of its Chinese iCloud users in China on a platform hosted by the state owned China Telecom.[49] To put Apple's arrangement in China in US terms, she describes it as if the US government required Alibaba to set up a data center under a new public private partnership in Alabama that is also subject to US military authority and oversight. She cites a similar hypocrisy of Google in refusing to work with the US military on facial recognition but willingly doing so with the Chinese government. Apparently China balances the requirements to store data in China with greater freedom for data aggregation and monetization (that would violate laws elsewhere) as well as financial incentives. Google should also be called out for refusing to help the American military but making its expertise in artificial intelligence available to the Chinese.[50]

These egregious practices violate the laws of the United States, not to mention the platform privacy policies to which millions of Americans agreed. Senators Josh Hawley and Tom Cotton have

---

[45] Fumiko Lopez v. Apple Inc. https://www.scribd.com/document/421179904/Fumiko-Lopez-v-Apple-Inc-Class-Action

[46] Kari Paul, "Google Workers Can Listen to What People Say to Its AI Home Devices," *The Guardian*, July 11, 2019, sec. Technology, https://www.theguardian.com/technology/2019/jul/11/google-home-assistant-listen-recordings-users-privacy.

[47] Kokas, Aynne, Cloud Control: China's 2017 Cybersecurity Law and its Role in US Data Standardization (July 26, 2019). Available at SSRN: https://ssrn.com/abstract=3427372

[48] *Schneier, Bruce (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company*

[49] "Apple's ICloud User Data in China Is Now Handled by a State-Owned Mobile Operator," *TechCrunch* (blog), accessed November 21, 2019, http://social.techcrunch.com/2018/07/17/apples-icloud-user-data-in-china-is-now-handled-by-a-state-owned-mobile-operator/.

[50] "Dunford: Google's Work in China Is Providing a 'Direct Benefit' to the Chinese Military," Task & Purpose, March 15, 2019, https://taskandpurpose.com/google-helping-china-military.

introduced legislation to address the problem of forced data localization and related issue.[51] They note the hypocrisy of American platforms which proffer to protect Americans' privacy with encryption and refuse to cooperate with American law enforcement but then are willing to provide the decryption keys to China. The bill would prohibit these practices by American firms in China and other countries that threaten national security. The bill also notes how Chinese government collects data on unsuspecting Americans through a series of equipment, products, and services, and the bill would prohibit the transfer of that information to China.

The unintended consequences of encryption

Encryption is a process of encoding information that only authorized parties can access it. While it does not prevent interference with data transmission, it can deny access to unauthorized parties. In response to backlash the platforms have received about their privacy practices, many have offered their users end to end encryption to avoid advertising tracking. Encrypted internet traffic has hit an all-time threshold of over 84 percent of all network traffic, up from 55 percent in 2017.[52] Moreover encrypted pages as a percent of browsing time is at 91 percent.[53] However, platforms have been less forthcoming about the fact that they collect information before encryption and after decryption, notably for advertising purposes.

Encryption is an important tool within larger suite of privacy and security technologies but should not be considered the privacy panacea. The key downside of encryption is that many of its most sophisticated users are criminals and sex offenders, and its proliferation makes its harder for law enforcement to do its job. The following example shows the unintended consequences.

An important point of control is the domain name server (DNS), the naming system for computers, services, or other resources connected to the internet or a private network. DNS is a worldwide, distributed directory service vital to the internet's functioning. Specifically, the DNS translates or renders a known domain names to a numerical IP address so that it can communicate with the larger internet. Google and Mozilla support a new protocol of encrypted DNS called *DNS Over HTTPS* or **DOH** which relocates that DNS resolution to a new part of the internet and brings increased control of the Internet under these already large entities. Normally, DNS is a separate service from the platform, but encrypted DNS demonstrates how platforms can also exert control on points outside their network

DNS is characterized as a feature of the decentralized and modular architecture of the internet. Many different entities provide DNS service, and it is at the forefront to fight cyberattacks, block malicious traffic, and limit the spread of child exploitation, terrorism, and other illegal activities. DNS is also the technology that allows parents to exercise controls to protect their children and families and a range of privacy-enhancing tools that are deployed today. DNS also enables the content delivery network industry. Until now, the control of this important part of the internet has been closer to the end user, but that could change.

Even though most of the internet traffic is already encrypted (and in large part with Google tools), Google has proposed encrypting DNS data for traffic handled through its Chrome browser and all Android devices, eclipsing current solutions users already employ. Under this proposal called DOH,

---

[51] S.2889 - National Security and Personal Data Protection Act of 2019 sponsored by Josh Hawley. https://www.congress.gov/bill/116th-congress/senate-bill/2889?q=%7B%22search%22%3A%5B%22hawley%22%5D%7D&s=4&r=1

[52] "HTTPS Encryption on the Web." Google Transparency Report. https://transparencyreport.google.com/https/overview?hl=en -. Last accessed October 28, 2019.

[53] Ibid

Google's operating system would see DNS data before and after it is encrypted. In doing so, Google could place itself at the virtual center of the Internet, with exclusive access to most DNS data. While we should encourage technological efforts to improve privacy, centralizing all DNS resolution with one entity potentially puts even more of the internet under Google's domain and dramatically changes the internet's decentralized character.

There may be reason for Google to offer encrypted DNS as a user option. However, setting it as a default setting raises significant concerns. Google has said it has no current plans to set encrypted DNS as a default setting on Chrome.[54] However, if those plans change, with a simple update to their code, Google can potentially bypass the user's local DNS and send encrypted traffic to the centralized Google DNS server instead.[55]

Mozilla also announced plans to implement DOH in the US in partnership with Cloudflare, though it claims to want to employ an experimental, stepwise test and learn approach.[56] Mozilla, of course, utilizes Google's Chrome browser.

Google and Mozilla[57] offer that the move is a mere default setting to which the user can opt out and that they offer parent DNS solutions and "safe search" options.[58] Undoubtedly, encrypted DNS makes business sense for Google and Mozilla, and some users may welcome the change. However, the furtive nature of the rollout appears to violate the spirit of the multi-stakeholder internet community. In the past Google and Mozilla would have engaged more directly with the multi-stakeholder approach. It may be that methods of DNS encryption are the inevitable next step for privacy, but the transition should be done more carefully and without trampling current tools which consumers and law enforcement use to protect the most vulnerable. Indeed, these concerns forced Mozilla to stop its encrypted DNS rollout in the United Kingdom. It begs the question of why American users aren't given the same consideration.

Security analysts have observed that centralizing even more traffic to Google's or Mozilla's (Cloudflare's) DNS creates a new but needless central point of attack, breaks many parental controls, disrupts enterprise content filtering solutions, and interferes with malware detection systems. Moreover, DOH can exacerbate challenges for law enforcement, which has hitherto relied on DNS information. When Mozilla acknowledges that DOH could "break" the content delivery network

[54] John D. MacKinnon and Robert McMillan. "Google Draws House Antitrust Scrutiny of Internet Protocol." Wall Street Journal. September 29, 2019. https://www.wsj.com/articles/google-draws-house-antitrust-scrutiny-of-internet-protocol-11569765637

[55] Google will conduct a limited DoH experiment in Chrome 79 in December 2019 and has committed to not change user defaults during the experiment. But Google has not yet made a firm commitment to do the same once the experiment is over and they deploy DoH more broadly.

[56] Selena Deckelmann, "What's Next in Making Encrypted DNS-over-HTTPS the Default," Mozilla, September 6, 2019, https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/; and Zak Doffman, "Firefox Plans Controversial New Encryption Setting for Millions, and Update Starts This Month," *Forbes*, September 8, 2019, https://www.forbes.com/sites/zakdoffman/2019/09/08/firefox-announces-major-new-encryption-default-to-protect-millions-of-users/.

[57] Over 90 percent of Mozilla's revenue comes from Google, as a result of the Mozilla Firefox browser setting Google as the default search engine. It is unclear what the terms of the agreement with Cloudflare are to make them the default DoH resolver for Firefox. Cloudflare has recently filed an initial public offering. See Stephen Shankland, "Google-Firefox Search Deal Gives Mozilla More Money to Push Privacy," CNET, November 27, 2018, https://www.cnet.com/news/google-firefox-search-deal-gives-mozilla-more-money-to-push-privacy/; and Jordan Novet, "Web Security Company Cloudflare Files to Go Public," CNBC, August 15, 2019, https://www.cnbc.com/2019/08/15/cloudflare-s-1-ipo-filing.html.

[58] Mozilla has created a "canary domain" concept so that networks can signal to the browser that content controls are in place so that centralized DoH is turned off, but Google has not developed a similar method.

(CDN) industry.[59] Stacie Hoffman, Digital Policy & Cyber Security Consultant at Oxford Information Labs Ltd., notes, "What is missing right now is a public discussion of the trade-offs between particular approaches to security (e.g. DNS encryption) with other security measures distributed throughout the Internet's layers (e.g. malware blocking in the network) and the wider effects on society."[60]

However, the lucrative new opportunities for global data monetization by large platforms is likely driving the current efforts. Google's future plans on this issue are not entirely clear, and it is not clear whether disadvantaged parties could take legal action against Google and Mozilla for an activity that turns off their traffic in an instant, but it exemplifies that vast power that can be wielded, outside of the platforms on points that are not even within their own network, with a mere coding tweak.

While ever more internet transmissions are encrypted to protect privacy, the rate of child sex abuse online has exploded *exponentially*. While it is not suggested that encryption causes child exploitation, the proliferation of the problem has reached unprecedented levels. Reports of suspected child sexual exploitation to the National Center for Missing & Exploited Children's (NCMEC) CyberTipline have increased 1.1 million in 2014 to 18.4 million in 2018 with an associated 45 million photos and videos of abuse. A recent *New York Times* series investigated the crisis, how law enforcement is ill-equipped to address it, and that technology companies efforts to stem the flow of the illegal content is weak and inconsistent.[61] Six Senators sent letters to Google, Amazon, Apple, Facebook, and other tech firms about their failure to take meaningful steps to stop the creation and sharing of child sex abuse material.[62]

Shortcomings of Proposed Regulatory Approaches

It is understandable that in the face of the problems posed by tech platforms, many have turned to the most drastic solutions. Indeed, the most drastic responses are now on the table because the platforms jettisoned the moderate, proactive solutions that would have likely forestalled the situation today. Already in 2012, President Barack Obama proposed a Consumer Privacy Bill of Rights whose principles are hardly controversial: individual control, transparency, security, accountability, and strengthened enforcement at the FTC.[63] The proposal supported using multi-stakeholder processes to develop enforceable codes of conduct through Section 5 of the FTC Act. Importantly, the Obama administration advocated the preemption of state laws that would contradict the national standard. It expected states to participate in multi-stakeholder processes and believed that states proposing more stringent requirements would diminish incentives for firms to adopt the codes of conduct. Moreover, the administration wanted Congress to codify forbearance

[59] DNS-over-HTTPS (DoH) FAQs. "Will DoH break Content Delivery Networks (CDNs)?" Mozilla Support page. https://support.mozilla.org/en-US/kb/dns-over-https-doh-faqs#w_will-doh-break-content-delivery-networks-cdns Accessed October 28, 2019

[60] Stacie Hoffman. "Recalibrating the DOH Debate." CircleID. July 23, 2019. http://www.circleid.com/posts/20190723_recalibrating_the_doh_debate/

[61] By MICHAEL H. KELLER and GABRIEL J.X. DANCE; Kholood Eid and Jack Nicas contributed reporting. Susan C. Beachy and Alain Delaquérière contributed research.. "Child Sex Abuse on the Internet: Stolen Innocence Gone Viral". The New York Times, September 29, 2019 Sunday. https://advance-lexis-com.zorac.aub.aau.dk/api/document?collection=news&id=urn:contentItem:5X57-VG31-DXY4-X176-00000-00&context=1516831. Accessed November 22, 2019.

[62] https://www.blumenthal.senate.gov/imo/media/doc/11.18.19%20-%20Google%20-%20CSAM.pdf

[63] White House Office: http://www.whitehouse.gov, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 23, 2012, https://www.hsdl.org/?abstract&did=.

from enforcement of state laws for companies already compliant with the FTC's codes of conduct.[64] Sadly, Silicon Valley players torpedoed the effort.[65] With the Obama Administration enmired in the Edward Snowden scandal, the European policymakers took the opportunity to claim the moral and political high ground and advanced the GDPR. The US missed the chance to set global internet norms, which historically it had succeeded to do.

As the control systems discussion identified, the risk to the privacy and security can increase because of the size and scale of the system. While such large enterprises have larger budgets to invest in these endeavors, the once size fits all approach was not tested, and moreover it falls hardest on small and medium sized companies which did not violate their customers' privacy. The GDPR, a solution based upon the leviathan bureaucratic state may allow government to extract payments from the platforms, but it fails to action the innovative capacities of the firm to improve their system or to encourage their users to behave differently. Instead it entrenches the status quo.

Constructing a privacy regulatory regime for online privacy is not easy, even if the focus is the large platforms. Privacy regulation requires a coherent identification of the problem, a description and quantification of the harm, a grownup assessment of the range of regulatory instruments, a discussion of how the proposed policy instrument will address the problem, and an independent way to measure whether and how the regulation is protecting privacy. This needs to be done without falling back on knee-jerk pronouncements that a solution is either total government intervention or complete laissez-faire in the marketplace. Few would disagree that big tech companies have broken the public's trust. All the same, government intervention struggles to create outcomes that improve upon the status quo.

Many have touted the CCPA, some calling it "GDPR-lite." However, the CCPA could be even onerous than the GDPR. Consider the following breakdown of the provisions of the two laws (Table 1).

Table 1. Breakdown of General Data Protection Regulation vs. California Consumer Privacy Act

GDPR	CCPA
173 recitals	185 provisions
45 regulations on business practices	77 regulations on business practices
43 conditions of applicability	47 conditions of applicability
35 bureaucratic obligations	17 bureaucratic obligations
17 enumerated rights	11 enumerated rights
11 administrative clarifications	17 administrative clarifications
9 policy assertions	6 policy assertions
5 enumerated penalties	10 enumerated penalties

Source: Author.

[64] Roslyn Layton, "A Look at the Growing Consensus on Online Privacy Legislation: What's Missing?," AEI, October 29, 2018, https://www.aei.org/publication/a-look-at-the-growing-consensus-on-online-privacy-legislation-whats-missing/.

[65] Natasha Singer, "Why a Push for Online Privacy Is Bogged Down in Washington," *The New York Times*, February 28, 2016, sec. Technology, https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html.

Some 40,000 internet startups in the US were founded in 2018 alone.[66] However, this a staggering number is likely to fall with the promulgation of the CCPA, what is more correctly called the GDPR-heavy because it adds 77 new regulations to enterprise, 22 more than the GDPR. The largest platforms would prefer to extend the GDPR to the US, rather than to adopt the CCPA, which has some overlapping but slightly different provisions.

The California Department of Justice and Office of the Attorney General recently issued a cost benefit analysis of the CCPA legislation and its own supplementary regulation. It notes the total initial compliance cost of $55 billion, 1.8 percent of California's gross domestic product in 2018, and another $16 billion in the coming decade.[67] About half of surveyed firms expect costs to run between $100,000 and $1 million, with vast majority of the fees going for legal services. The report also notes that 99 percent of California companies have fewer than 500 employees, meaning that costs will fall hardest on the firms with the least amount of resources and employees.[68]

Even with sophisticated modeling and economic projections, there are no scenarios in which benefits either meet or exceed costs with the CCPA. The most generous models suggest consumer benefit could amount to $1.6–$5.4 billion over time based on experiments in which consumers report willingness to pay for privacy features. Other cost benefit models suggest conservatively that the costs of the CCPA exceed benefits by a factor of four.[69]

As such, the policy will be a drag on the economy and is likely to hasten the SME exodus from the state. For a state that bills itself as a progressive leader, California is transferring massive wealth to the privacy and plaintiff bars, key advocates for the CCPA. If the goal was to help consumers, then it would be better to provide rebates to customers than fees to lawyers. The report reiterates the findings of the GDPR with the expectation of a similar impact with the CCPA noting,

> Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises. Conventional wisdom may suggest that stronger privacy regulations will adversely impact large technology firms that derive most of their revenue from personal data, however evidence from the EU suggests the opposite may be true. Over a year after the introduction of the GDPR, concerns regarding its impact on larger firms appear to have been overstated, while many smaller firms have struggled to meet compliance costs. Resources explain this dichotomy as large technology companies are often several steps ahead of both competitors and regulators.[70]

When startups and small players exit, existing large companies which can afford to comply will take the market share of the firms that exited. This is what happened in the EU and is what will happen in

[66] TIA Cyberstates 2019

[67] Berkeley Economic Advising and Research, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," State of California Department of Justice Office of the Attorney General, August 2019, http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

[68] Ibid p. 31

[69] Roslyn Layton. "The costs of California's online privacy rules far exceed the benefits." AEIdeas. March 22, 2019. https://www.aei.org/technology-and-innovation/the-costs-of-californias-online-privacy-rules-far-exceed-the-benefits/

[70] Supra Berkeley p. 31

California if the CCPA is not preempted. Academic studies of other industries over time have noted that entry regulation is a barrier to entrepreneurship.[7172]

Not only can complex regulation reduce enterprise, it can trick consumers into believing the marketplace is trustworthy. Indeed "complex regulatory frameworks create the illusion of a well-controlled system," notes a recent report of Scientific Board of the European Financial Systemic Risk Board.[73] Similar unintended consequences have been noted in other industries, particularly banking and finance as the report describes,

> Excessively complex regulations contribute to increased systemic risk in several ways. First, complex regulatory frameworks create the illusion of a well-controlled system, while at the same time creating incentives for regulated entities to game the system. Second, such a framework risks missing contingencies that are not well understood, e.g. because of a lack of historical experience. An "over-fitted" regulatory system may not be well equipped to address "unknown unknowns". Third, when risks materialize, the combination of hard-to-understand interactions between different regulations and a wide array of regulatory tools can make policy responses convoluted and difficult to judge. It can also hamper the accountability of regulators and supervisors. Finally, excessive regulatory complexity can encourage the transfer of risks to institutions outside the regulatory perimeter, creating an environment where systemic risk is amplified more than it would have been if risks had remained within the perimeter.[74]

Even before the CCPA California already had privacy regulations across a range of field than any state. It is not clear that Californians felt any more private or safe as a result.

A leading Santa Clara University law professor and more than 40 California-based privacy professionals and lawyers attest to the rushed, sloppy process in which the California legislature wrote the CCPA in a mere week.[75] Moreover, the GDPR's grab bag of provisions and asserted rights do not cohere to scientific standards of building trust online.[76] There was no evidence-based process, split testing, or trials to develop the many provisions of the law; rather, stakeholders each tacked on their favorite talking point. Indeed a separate, independent test of the various asserted rights found that users value the provisions differently than do lawmakers—and certainly not equally as the law is written.[77] It appears that California policymakers attempting to be even more "woke" than their European counterparts, proffered additional requirements to one-up the Europeans, for example the requirement that every website post a 1-800 number for users to call to make privacy requests and complaints.

A separate analysis show that CCPA implementation costs are at least $100,000 per firm. This

---

[71] Klapper, L., Laeven, L., & Rajan, R. (2006). Entry regulation as a barrier to entrepreneurship. *Journal of financial economics*, *82*(3), 591-629

[72] Kotsios, P. (2010, March). Regulatory Barriers to Entry in Industrial Sectors. In *International Conference on International Business*.

[73] "Regulatory complexity and the quest for robust regulation." European Financial Systemic Risk Board. Reports of the Advisory Scientific Committee. No 8. June 2019.

[74] Supra p. 2

[75] See Eric Goldman, "An Introduction to the California Consumer Privacy Act (CCPA) (July 9, 2018)," Santa Clara University, https://ssrn.com/abstract=3211013.

[76] Roslyn Layton, "How the GDRP Compares to Best Practices for Privacy, Accountability and Trust," March 31, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944358.

[77] Sabolewski, Maciej and Palinski Michal. How much consumers value on-line privacy? Welfare assessment of new data protection regulation (GDPR). International Telecommunications Society Conference, Passau. July 31, 2017

suggest that the costs of the CCPA will exceed benefits by a factor of four.[78] As detailed in insightful research by the Rand Corporation's Sasha Romanovsky, there are but a few hundred privacy violations in the US annually, and the economic costs of harm are unknown.[79] Given the scale of trillions of interactions annually, that there are only few hundred privacy violations suggests that the incidence of violation is low. While no one desires their privacy violated, that the actual harm has not been identified or calculated suggests that it is not very high. This also suggests that it is logical to focus on the largest platforms to most effectively remedy the problem.

Policy Solutions

There is a false choice that online privacy governance must either be the seeming EU leviathan state (social control with an absolute sovereign) or a seeming US free market (no government intervention). Over time, the US has implemented many rules to protect individuals' information from overreach by the administrative state while recognizing the benefit of some information being in the public domain (e.g., phone numbers and addresses in telephone books, subject to opt out for a fee). Hence, policy has generally promoted the importance of trust, a confidence in the reliability of a system, rather than the absolute right of an individual to seclude information about oneself.

Over time a system to analyze risk emerged, and, recognizing the sensitivity of certain information, rules were adopted to manage sensitive data, notably that of children, health, and finance. Meanwhile, other sectors and industries remain subject to discipline based on actual harms and tests for unfairness and deception. This framework of permission-less innovation has been important for consumers and entrepreneurs. It does not assume that every collection of data is suspect. Instead, it focuses scarce regulatory resources to the areas where it's needed. Permission-less innovation has allowed America's internet economy to emerge and flourish. It's not the same in the EU, where individuals have many regulatory barriers just to get out of the gate.

Following in this vein it is logical to evolve a new regime that focuses on the discrete large players because of the increased risk posed to individual privacy because of the size and scale of the enterprise. The remaining online firms, for which there are many millions, they continue to be subject to existing privacy laws and they can transition to a set of certifiable technical standards described below.

A critique of FTC enforcement is that it is too slow. It should be noted that FTC enforcements are done carefully and systematically to ensure that they are correct and defensible under the law. Moreover, nearly all regulatory action is subject to legal challenge, a due process principle enshrined in Constitution and sector specific law. Notably FTC enforcements of the tech companies have been conducted faster than GDPR enforcement, which was described at the outset to take two years and is also subject to court challenge. As shown, US regulators can exact significantly larger fees and conduct relief than Europeans. The FTC could certainly be strengthened with greater budget to employ more economists, technologists, engineers, and case works to enforce the privacy laws.

Certifiable technical standards of privacy and data protection

University of Washington Professor of Law Jane K. Winn offers a framework of information governance that addresses privacy and disclosure in a flexible, dynamic way and path forward for

[78] Roslyn Layton. "The costs of California's online privacy rules far exceed the benefits." AEIdeas March 22, 2019. http://www.aei.org/publication/the-costs-of-californias-online-privacy-rules-far-exceed-the-benefits/

[79] Sasha Romanosky, Policy Researcher, RAND Corporation. The Empirical Economics of Privacy and Data Security: What Do We Know, and What Do We Wish We Knew?. https://web.cvent.com/event/425f4add-7433-4631-b002-f8202771a675/summary

Congress on privacy legislation.[80] She suggests building the regulation from the bottom up by working with consensus standards organizations to create concrete, certifiable standards for the specific business practice in question. Unlike industry self-regulation, "accredited" standards are certified by the American National Standards Institute and organizations adopting these official standards must observing the due process requirements contained in a document known as "ANSI Essential Requirements." ANSI standards are already employed today and are difficult to obtain. Compared to the EU's fundamentalist approach, technical standards are explicit and measurable and therefore can ensure stricter compliance. Moreover, they offer the benefit of transparency. Instead of waiting for the regulator's interpretation, any person can review the standard and see whether the firm is upholding it. She also describes how Congress can enable the transition for the millions of firms to which the integrated, national information framework would apply, Congress could authorize federal regulators to confer "safe harbor" status to organizations adopting the rigorous standards along with limited preemption for inconsistent state laws.

This paper briefly reviewed the outcomes to date of the GDPR and the expectations for the CCPA. It describes why online platforms are unique entities of unprecedented size and scale which require the appropriate description and oversight. It demonstrates the folly of constructing a model and associated regulation based upon a view that every firm is the equivalent of Google. Moreover, it describes why the all-data-is-equal fundamentalist approach has strengthened the largest players to the detriment of small and medium sized ones. The GDPR, however well-intentioned, has not succeeded to increase users' trust online or encouraged broad compliance. Moreover, with detailed discussion of the privacy violations of the large platforms, the paper shows that the GDPR and CCPA will not necessarily address or deter the problems. The paper introduced the concept of certifiable technical standards for data privacy and protection as an effective regulatory alternative which builds on America's 200 year tradition to protect individual privacy while complementing, not dismantling as the CCPA will unwittingly do, the many existing laws, structures, and institutions created to protect privacy . The paper contributes to the policy research field with further discussion of the impact of platforms, comparative analysis of data regulatory regimes, and policy recommendations to update state and federal data privacy rules for the online economy.

[80] Winn, Jane, The Governance Turn in Information Privacy Law (July 11, 2019). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3418286