Regulating Online Privacy: Some Policy Guidelines, Including Guidelines for International Harmonization

Eric K. Clemons
The Wharton School
clemons@upenn.edu

Jordyn Benattar
The Rotman School
jordyn.benattar@mail.utoronto.ca

Abstract

With dramatic changes in technology capabilities, much of current privacy law in the US and abroad has been rendered out of date. Analogies and precedents are difficult to interpret, leading to decisions that are inconsistent, problematic, or wrong. Searching the text messages on an iPhone is not *the same as overhearing a conversation. Searching an entire Facebook account for evidence of fraud is* not *the same as searching a bank account. We review the lessons of four current court cases involving online privacy and develop a set of guidelines that could be used to develop coherent privacy policy. The guidelines were developed with the expectation that they could confer no advantage on firms in nation, and that they would provide all citizens with the privacy protections no less than those they enjoy in their home countries.*

1. Introduction to the Problems in Regulating Online Privacy

Technological innovations are occurring at an unprecedented rate. These innovations expand the capabilities of individuals and legitimate businesses. They also expand the capabilities of terrorists, terrorist cells, and criminal organizations. And they expand the capabilities of governments, both friendly and hostile, foreign and domestic. This alters the nature of threats we all face, as well as the need for speed to detect and prevent them. Augmented capabilities and changing nature of threats requires a coherent response in public policy, regulation, and law. This coherent response must be agreed both at home and abroad, and coordinated with both foreign and domestic governmental agencies. This challenges traditional regulatory frameworks and limits the applicability of historical analogies and legal precedents.

The United States needs a new and clear privacy policy based on current technological capabilities, current needs for legal protection, and current business models and business practices. We need a privacy policy based on the business environment as it exists today and as it is likely to develop in the foreseeable future. A privacy policy based on historical precedents and imprecise analogies will lead to legal decisions that are poor and are inconsistent across jurisdictions domestically and internationally. These decisions will be based on the idiosyncratic selection of examples and analogies offered in each dispute, and on the responses of individual courts.

We need a clear new privacy policy, to protect individuals, to guide the courts, and as importantly to protect American corporations and guide their strategic planning efforts by removing an enormous source of uncertainty. Privacy policy has multiple objectives, which sometimes conflict with each other. Making it harder for governments to "crack" encryption protects individual privacy by making arbitrary search by governmental agencies more difficult. However, this also makes it more difficult for governments to detect and monitor terrorist activities and thus makes it more difficult to prevent terrorist attacks.

Moreover, we need a clear new privacy policy that is harmonized globally. There are many reasons why global harmonization is required. Individuals need to understand their rights and the protections available to them both at home and abroad. American corporations should not placed at a competitive disadvantage by the US imposing more stringent requirements on data sharing with law enforcement and government agencies than those that are imposed on foreign corporations. European corporations should not placed at a competitive disadvantage as a result of unequal enforcement of privacy laws, which allows American firms to operate in Europe in ways that are both spectacularly profitable and illegal for European corporations.

We begin by explaining why it is necessary to change our regulatory regime. Section 2 explains the importance of a new policy based on current technological capabilities, since existing regulations do not address contemporary business practices. Section 3 lists the objectives that we believe should guide the redesign of domestic American regulation. Section 4 explains that the problem is not new; regulatory change frequently lags technologic evolution. Section 5 reviews why this truly is a problem, by exploring the difficulties encountered when using historical precedent to resolve conflicts in the use of modern technology. Section 6 reviews *The Big Four* in current privacy litigation, cases involving Apple, Microsoft, Google, and Facebook, which are without a doubt the four largest providers of online software in the western world. Section 7 provides some guidelines for developing new privacy policy, while section 8 provides our suggested policy. Finally, section 9 provides brief conclusions.

2. The Importance of a Clear New Policy Based on Current Technological Capabilities and Current Business Practices

Whenever possible regulation should be based on historical precedents. American jurisprudence is based

URI: http://hdl.handle.net/10125/50556
ISBN: 978-0-9981331-1-9

on constant evolution, as new situations arise, new business practices arise, and new sources of conflict and litigation arise. Historical precedent does not prevent evolution, but it places clear and deliberate limits on the pace of change, providing stability, predictability, and in most cases fairness.

However, discontinuous change in technological capabilities and in the business practices that they enable do, indeed, create discontinuous changes. We start by using well-known examples not selected from the privacy domain. None were anticipated when the original regulations were drafted, and, similarly, all entail possibilities that were not envisioned and were not relevant during the litigation of prior cases. Some practices that might have been deemed as abusive in earlier cases may not be abusive today. When there were only three television networks, and a region might have access to at most three stations, the Fairness Doctrine [10] was essential to ensuring that all citizens had access to sufficient sources of information. With literally hundreds of broadcast and online sources of information today, the Fairness Doctrine is no longer as critical. In contrast, the First Amendment to the American Constitution [12], perhaps the most important of the amendments in the Bill of Rights, places virtually no restrictions on freedom of speech. The Founding Fathers, the drafters of the American Constitution, were concerned with the ease with which a government might silence all opposition by seizing printing presses. They did not envision the ease with which illegitimate voices, including agents of foreign powers, might flood the US with online fake news. Nor did they anticipate the speed with which fake news from legitimate American sources might be picked up and amplified, and used to distort elections or to deliberately misinform the public. Lying for political advantage is not new. But the speed with which technology can spread and amplify lies is unprecedented.

Discontinuous change in business practices has always resulting in discontinuous change in regulation. Small local proprietors could not influence the supply or prices of most goods, and the invisible hand of the market was quite sufficient to ensure efficient operation, and to regulate supply and prices of both goods and labor. In contrast, when the industrial revolution facilitated the emergence of massive vertically and horizontally integrated corporations, antimonopoly laws and antitrust laws become essential to protect both consumers and the competitive environment. Small local producers sold their goods to their neighbors. Defective products, and most importantly, dangerous and unwholesome products, were more readily detected, despite legends such as the tale of Sweeney Todd. Mostly, you could not get away with selling spoiled meats or contaminated milk to your neighbors. Massive industrial manufacturing facilities, selling to communities hundreds, or even thousands of miles away, required inspection, resulting in the creation of the Food and Drug Administration in 1906 [13]. Additionally, small local producers sold their goods to their neighbors, and deceptive advertising and deceptive trade practices were readily detected. In contrast, broadcast advertising created new opportunities for deceptive claims, resulting in the creation of the Federal Trade Commission in 1914 [11].

Technology has created situations that never existed before, creating legal paradoxes that never existed before. Current law prohibits mail carriers from reading the contents of first class mail, and current practice prohibits common carriers like Federal Express and DHL from opening sealed communications. In contrast, there are few legal restrictions what Google or other email service providers can do with the contents of private messages that they deliver. Moreover, the regulation of these paradoxes is not consistent and is not always in the best interests of consumers. The Japanese Constitution protects consumers from their telecommunications providers performing any form of data mining on the content of the users' communications. There were no such restrictions on Google as an email provider or search provider, because when the Japanese Constitution was drafted after World War II neither email nor online search was anticipated as potential threats to individual privacy. Decades later Google was of course unregulated in Japan. Yahoo!, which was owned by a company that also provided wireless telecommunications services, had numerous restrictions on how it could use its users' content for commercial purposes. Rather than restrict Google to bring it in line with the intent of the framers of the Japanese Constitution, the restrictions of Yahoo!'s owner, Softbank, were dropped. It is hard to imagine how this could be best for Japanese consumers [36, 39].

It is also clear that current technology has created threats to privacy of a scale that has never existed before. It is clear that online data integrators have prepared more complete profiles on individual consumers, their expected cost to serve, their expected willingness to pay, and all aspects of their purchasing behavior [14, 21, 41]. It has been shown by Ben Shiller [35] and others that this information has now starting to be used to increase the prices charged to specific, identifiable, individual consumers.

Moreover, the legal remedies that have been offered do not address the problems of informed differential pricing adequately. The Electronic Communications Privacy Act (ECPA) of 1986 was intended to provide the same degree of privacy protection for email and other forms of electronic communications that already existed to protect privacy from wiretapping [8]. Unfortunately, voice communications are transient; you say something, and if it has not illegally been recorded it is gone. In contrast, email can remain in storage indefinitely. In the more than 40 years since the act was drafted, our use of email has changed dramatically; it is no longer analogous to 1986

use of telephony, nor is it analogous to our use of traditional mail. The bill is seriously outmoded [1, 11]. Many of the disputes that we discuss in section 6 are in large measure based on different interpretations of the ECPA. The digital right to be forgotten online has been suggested as a mechanism to protect consumers from the negative impacts of data mining and from the negative impacts of inaccurate or irrelevant information [32]. Some form of the right to be forgotten has already been introduced in the EU and South Korea, and several other jurisdictions are considering introducing additional measures. While the right to be forgotten does allow individuals to delete links to information stored online, so that they do not appear in search results, the original articles still remain accessible on the net. More relevant to the issue we are discussing here, data warehousing does not involve doing a search for archival information. Rather, it involves tracking your transactions, in real time, as they occur, and integrating them across the broadest possible range of sources. Removing links to one or two articles will have no impact whatsoever on data mining, data integration, and data warehousing. It will have no impact on privacy violations, or on the financial costs associated with precision pricing enabled by privacy violations.

The capabilities of data analysis, especially machine learning and big data analytics, are barely understood by experts today. They clearly were never anticipated by prior legal scholars and they clearly are not covered by historical legal precedent. Analysis of Facebook "likes" has been shown to be sufficient to infer vast amounts of information with a surprisingly high degree of accuracy, including assessing personality traits [22, 27], and the ability to determine birth gender and sexual orientation, religion, and political affiliation. Similar uses have been found for other sources of public information, even of the photo you select for your Facebook wall. This can be combined with data warehousing and used in an ever-increasing variety of ways. Not all of the uses are beneficial to consumers. Documented commercial uses include discriminating against renters based on race or religion, discriminating in coverage availability or prices for insurance applicants, and precision targeted marketing to children [6, 7, 30, 40]. Equally troublesome is the potential for election manipulation, as indicated by recent experience with the Brexit campaign and with Trump's recent presidential campaign [3, 37].

Most current corporate practices that address privacy are based on outmoded regulations, and when modern corporate strategy and online business models are regulated by rules developed in the 1960s or 1980s the results are less than ideal for consumers. Attempts to regulate one corporation by analogy with another in a different industry, or with a regulatory policy designed for a different era, are unpredictable. Google is permitted to read email, in ways that no carrier of traditional mail would be permitted. Google is permitted to view your purchase history and use it commercially, in ways that no credit card issuer or financial services firm would be permitted to do. Google and Uber are permitted to monitor your geographic position constantly, with persistence that would not be permitted for any employer, and indeed would not be permitted for law enforcement agencies without a court-ordered tracking device. And yet each of the examples involves firms with only a limited slice of the data available on any one of us. Moreover, each of these firms has a sound business reason for wanting the data they are gathering. Google does not charge consumers for services they provide, and their use of private information they capture is the basis of the bulk of their profits. Uber could not predict demand as well, and could not dispatch cars as quickly, if it did not know the location of its passengers. In contrast, local internet service providers (ISPs) are now permitted to view, store and analyze any and all data that they transmit and to use it for commercial purposes, as a result of recent bill passed by the US Congress [15]. In theory, without clarification and without modification, this bill would allow your ISP to combine financial services data, texting and email, transmission of documents and photographs for storage in the cloud, search history, and medical records sent to you through secure portals, to create a portrait of you in unlimited detail. This is permitted, despite the fact that it is far broader than the data available to any other commercial enterprise. This is permitted despite the fact that your ISPs have numerous other sources of revenues and of profits. Google is not the right corporate analog for regulating Comcast and Verizon as ISPs.

3. Objectives of American Regulation

We see at least six objectives for privacy regulation in the United States. Each objective seeks to protect a different constituency.

Protecting the privacy of our citizens as guaranteed by the Fourth Amendment to the US Constitution, prohibiting illegal search and seizure. The Fourth Amendment guarantees that in their homes Americans are safe from search and seizure of property by the federal government, unless the government can show cause and can obtain a valid search warrant. By extension this now applies to search and seizure by state and local governments. Government surveillance of our online activities should be governed by the same rules that govern search of our physical property, our mail, and our traditional telephony.

Protecting our citizens by apprehending and convicting traditional criminals. The need to respond immediately to perceived terrorist threats may sometimes require that the courts provide sweeping investigatory powers, including electronic surveillance of a suspect, all of his electronic communications, and the electronic communications of all of his or her contacts.

Protect the privacy of our citizens by not setting precedents that place them at risk from illegal search by foreign governments. If the access that the US government demands from US online service providers are too great, this may create precedents that can and will be used by foreign governments to demand corporate cooperation with their own surveillance activities. If the US can force an American company to violate the norms of the countries in which it operates and to provide data on foreign nationals in order to obey the wishes of the US government, does this set precedents for foreign governments to demand similar concessions when investigating US citizens?

Protecting the state from the activities of terrorists and enemies, foreign and domestic. Sometimes the US will need to access data quickly to prevent a terrorist attack, or to prevent the destruction of evidence related to a past or planned future attack. While suspected terrorists have rights in the US, for example if they are US citizens, the courts should be prepared to provide access to critical information almost immediately.

Protecting the interests of American corporations by not placing them at a strategic disadvantage relative to foreign competitors. If Microsoft and Google email accounts are seen as unsafe for foreign nationals, this will accelerate the growth of non-US competitors, including those who would not normally be able to compete with Microsoft and Google either in terms of price of services or in terms of service quality. Given the importance of high tech service providers to the US economy and to the US balance of trade, actions that increase the attractiveness of foreign competitors can hardly be seen as in the best interests of the US. Facebook is thriving in the EU despite repeatedly violating EU privacy policies. If these consistent privacy violations were seen as somehow supporting activities of the US government it is not clear that the population of the EU nations would be as tolerant of them. This one of the few scenarios that could lead to replacing Facebook in Europe with one or more local and locally regulated alternatives.

Protecting the privacy of foreign nationals from illegal search and seizure enabled by precedents established by US law enforcement. If the US can demand access to data on US citizens, regardless of where the data are located, and irrespective of the local policies on search and privacy in the countries where the data are located, then foreign governments can do the same. A citizen who resides in the US and uses US software providers might previously have felt secure from illegal search and seizure. However, if the US can demand that service providers deliver information on its citizens regardless of where they or their data reside, presumably any other nation could do the same.

4. The Problem Drafting Appropriate Regulation Is Not New — Regulation Frequently Lags Technological Innovation

Technological innovation has frequently demanded a reexamination of privacy policies, and of regulation more generally.

American jurisprudence is based on historical precedent and analogy, as well as law. That is, precedent and analogy go a long way towards governing the interpretation of law. But analogies are imprecise, and on occasion can lead to absurd decisions when using them to interpret the application of old law to new technologies.

It is generally accepted in American courts that no warrant is needed when overhearing unguarded speech over a cellphone. If a suspect says something out loud, in public, in the presence of a police officer then no warrant is required to "capture" that speech as evidence. The State of California tried to argue, in Riley v. California, [33], that by analogy the police did not require a warrant to view the text on a suspect's cellphone during an arrest. Ultimately, after rounds of appeals, the case was decided by the US Supreme Court. The Court ruled that while a casual observer can overhear speech, and there is no presumed right to privacy when speaking in public, a casual observer cannot read your texting history when you carry your phone in public [2, 29]. Thus, a warrant is required to search a suspect's cellphone. However, while the ruling seems self-evidently correct, this dispute actually reached the US Supreme Court before it was resolved. Analogies, in the hands of skilled lawyers, are complex things and their interpretation can be unpredictable. Regulatory clarification would help make clear what analogies are correct and what are not, and where precedents are applicable and where they are not.

Problems with applying existing regulations and historical precedents to unfamiliar technology are not new nor are they restricted to privacy. The evolution of attempts to regulate AT&T over several decades provides an instructive early example. AT&T was a natural monopoly, perhaps the first significant natural monopoly in business history. The more people connected to a network the more valuable the network becomes; AT&T offered our first example of a positive participation externality, also called a network effect. Moreover, with the more limited technology of the late 1800s and early 1900s, people connected to a different network, one not operated by AT&T, could not communicate with people on the AT&T network. Clearly, the bigger the AT&T network became the more valuable it was to AT&T's customers. Just as clearly, customers who were on competitors' networks could communicate with fewer people, could not communicate with the majority of Americans, and received less value, even though their services cost as much to provide. Thus, the fewer competitors that

were operating in the US, and the more people who relied upon AT&T for their telecommunications services throughout the US, the better off everyone would be. It was not immediately clear how to deal with a natural monopoly. Natural monopolies were not covered adequately by either the Sherman Act (which focused on heavy industry) or the Interstate Commerce Act (which focused on rail networks rather than telecoms networks). The Sherman Act was intended to prevent abuse caused by huge industrial monopolies by limiting their growth and their increase in market share. But with the telecommunications technology that existed at the time, communications across the boundaries of an individual company was impossible. Hence the US actually needed and wanted a telecommunications monopoly. The Interstate Commerce Act was designed to prohibit abuse of farmers and rural shippers by prohibiting abusively high prices on short haul traffic over monopoly lines; a farmer's cost for the first few miles shipping produce to Chicago might be as high or higher than the cost of shipping it the rest of the distance to New York [16]. There is no indication at AT&T was abusing local service customers in order to facilitate long distance communications. Indeed, AT&T was overcharging for long distance communications (long haul) and undercharging local service customers (short haul), the very opposite of the problem that the Interstate Commerce Commission was created to address. AT&T was subsidizing local subscribers, in order to achieve the socially desirable goal of universal service, or universal access to the telecommunications network. While it was clearly socially desirable to move towards universal service, this, too, grew AT&T's market share and strengthened AT&T's monopoly position. When neither the Sherman Act nor the Interstate Commerce Act were appropriate for regulating AT&T the Justice Department turned to AT&T itself for guidance. The result was the Kingsbury Commitment [41] of December, 1913. This recognized AT&T's role as a natural monopoly and indeed did nothing to weaken AT&T's monopoly power or reduce its market share. Instead, the Kingsbury Commitment merely required AT&T to divest Western Union (the telegraph company) and required it to stop acquiring small local telephone companies; in exchange it was given complete control over its operations, subject only to a constraint on its total profitability. Unlike the UK, where telephony became a division of the national postal service, in the US AT&T retained its status as a publicly traded company, subject to rules that limited the financial impact of its monopoly power.

The next question regulators faced, two decades later, was how to deal with platform envelopment after AT&T moved into network broadcasting. Platform envelopment occurs when a company has significant power and significant market share and profits from one software element, usually an operating system or other extensible platform. Platform envelopment entails integrating a sequence of additional, complementary software elements. When the integration is done properly, the collection of elements has far more value than the sum of the individual values. Moreover, when done properly, the integrated collection cannot be duplicated by other vendors because they lack one or more critical components, such as Microsoft's control over the desktop through Windows, or Google's control over the cellphone desktop through Android. The user receives significant benefit, of course, which appeals to regulators. Competitors can be excluded, even destroyed, which regulators abhor. Markets alone cannot determine how to restrain platform envelopment. Platform envelopment was not envisioned when the Sherman Act was drafted. When AT&T launched America's first commercial radio station, and began to expand it to create America's first commercial broadcasting network, its control over long distance communications would have allowed it to block any other commercial broadcasting network. This was the eventual justification for the creation of the Federal Communications Commission, and for forcing AT&T out of network broadcasting [41].

5. The Big Four of Current Privacy Cases

There are four recent cases involving disputes between the US government, the FBI, the Department of Justice, or other law enforcement organizations, and the some of the world's largest and most important manufacturers of computer hardware or providers of computer software.

The simplest case to resolve was a dispute between the Department of Homeland Security and Apple, over unlocking the iPhones of two dead terrorists. A Federal judge in California ordered Apple to help the FBI access the contents of San Bernardino shooter Syed Farook's iPhone [23]. Apple refused, and their CEO Tim Cook vowed to resist the court order [24]. Attempts to bypass Apple's security are now risky, since the phone automatically erases the phone's data after too many unsuccessful attempts to unlock it. Clearly the case is complex because of the need to balance competing interests; in this case any decision would need to balance protecting US citizens from further terrorist attacks, which might have been imminent, protecting US corporations from the perception that their customers' data are readily available if the Courts in the US demand it, and the need to protect foreign nationals, whose own privacy might be placed at risk by establishing the precedent of letting governments demand access to phone data. Because of the threat to US corporations, Google's CEO publicly supported Apple's position in this case [18]. The case was easy to resolve only because the FBI was able to find experts who were able to crack the phone for them [31]. The dispute between corporate CEOs and the FBI attempts to balance the needs of national security on the one hand against the corporate needs for

commercially viable practices that protect individual's legitimate need for privacy. However, since the case was never resolved in the courts, no legal precedent has been established.

The dispute between Microsoft and the Department of Justice, over searching email stored in Ireland using only a US Warrant, is more complex, and indeed is still unresolved [4]. The case turned on the need for a valid Irish search warrant when searching the email of an Irish national drug dealer whose records are controlled by Microsoft and stored in Ireland. The DoJ argued that it did not matter where the data were located, and that as long as Microsoft controlled the data, anywhere in the world, it could be compelled to produce the data for search. Microsoft argued that although the data were in electronic form, and subject to their control, the emails could not be produced without a valid Irish search warrant. In 2016 Microsoft appealed, arguing that although the data were in electronic form, demanding that they be produced for US inspection was entirely analogous to the courts attempting to search a customer's paper files stored in a Citibank safety deposit box in Ireland with nothing but a US warrant. The 2nd Circuit Court of Appeals decided that if the data were in Ireland, an Irish search warrant was necessary. More recently, the same court rejected a request from the Department of Justice for an *en banc* rehearing of the case ["2nd Circuit denies rehearing in Microsoft Ireland case by an evenly divided vote [19]. Once again, the decision balanced an individual's rights to privacy, the US legal system's rights to fully informed prosecution, the competitive positioning of US information service providers, and the implications for foreign nationals. Since the US Department of Justice plans to appeal this case to the US Supreme Court, it has yet net been fully resolved.

The dispute between Google and the FBI is more complicated than the dispute between the Department of Justice and Microsoft. The FBI demanded that Google produce a large set of emails, and Google refused to provide some of them, arguing that the data might not be stored in the United States at any given time and that they could not be compelled to produce the emails solely on the basis of a US search warrant. They also cited the recent decision of the 2nd Circuit Court of Appeals, ruling in favor of Microsoft. The decision reached in the dispute was the opposite of the decision in the Microsoft case, and has the potential to create a contrasting decision that could limit the applicability of the Microsoft case. Magistrate Judge Thomas Rueter of The US District Court for the Eastern District of Pennsylvania used two arguments to justify finding a decision counter to the precedent of the Microsoft case [20].

The first argument hinged on the nature of Google's decision on where to store individual email messages in the cloud. It would be difficulty or even impossible to determine which valid search warrant or warrants are required when searching the email of American nationals, accused of crimes committed in the US, when even Google does not know where the data are stored. This argument also makes clear that storing the data of an Irish national in Ireland is fundamentally different from storing the data of a US national anywhere and everywhere, and this could be done explicitly to make search impossible.

The second argument appears, on its face, to be clearly absurd. Judge Rueter argued that it does not matter how the FBI obtains the emails that it demanded, and it does not matter from where in the world the data were obtained, because the data are not going to be examined until they reach the US. There thus would be no privacy violation and no illegal search or seizure, because the data are not obtained by the FBI until they have reached the United States. Thus by definition there is no illegal search because no privacy is violated until the data are examined in the US, where the warrant is legal.

Both Google's argument and the decision of Judge Rueter would provide dangerous precedents if upheld. Google's argument, if accepted, would allow software companies to avoid all warrants simply by moving data throughout the cloud constantly, so there is no single place to search and no warrant or set of warrants that would compel the company to submit the data that had been demanded. Judge Rueter's second argument, if accepted, would allow US courts to perform search and seizure, anywhere in the world, as long as the documents were not examined until they reached the US, even if these searches were illegal in the jurisdictions in which they were performed. Indeed, by extension, US agents could seize physical documents from a locked deposit bank or safe anywhere in the world, provided they had a warrant in the US, and provided no one looked at the documents until they had arrived in the US.

The current litigation involving search of Facebook data is fundamentally different from the other cases, because Facebook's argument is not that the warrant is illegal because of the location of the data but because of the scope of the court's request [28]. Quoting from the decision, *"In July 2013, [New York State] Supreme Court issued 381 warrants directed at Facebook upon a warrant application by the New York County District Attorney's Office that was supported by an investigator's affidavit. The warrants, …, sought subscriber information and content from numerous user accounts … ."*

This was a request for all the data on these 381 Facebook accounts, including friends lists, photographs, postings, and virtually all data associated with each account. In general, a search warrant needs to be specific about what the object of the search is, and what the authorities expect to find. This request was so broad that Facebook felt that it was more like a subpoena, a request to produce everything that might be relevant. However, while subpoenas can be challenged, search warrants cannot. The article in the

New York Times explains: *"But Judge Leslie E. Stein, writing for the majority, said state courts had held for decades that search warrants issued by judges cannot be appealed to a higher court. Instead, they may be challenged by a defendant only during a pretrial hearing, as illegal searches."* Since the judge held that warrants can't be appealed, the court therefore did not need to rule on Facebook's central argument, that the warrants were so broad that they should have been viewed as unconstitutional search.

Lower courts had argued that "Facebook, as a service provider, could not argue the searches were unconstitutional on behalf of its clients, any more than a landlord could stop the police with a warrant from searching a storage facility. Since the court did not rule on Facebook's argument, this leaves unresolved the issue of just how broad and invasive an electronic search can be. Searching an individual's safety deposit box for specific documents can produce at most a limited amount of information, which must be covered by the warrant to be used as evidence. Searching an individual's hard drive for specific information, likewise falls within the scope traditionally permitted for a warrant. Searching an individual's Facebook account for *everything* accessible may represent a substantial deviation from the scope of traditional warrants.

Only the Google case and Facebook case appear to create interesting and potentially problematic precedent. Both cases suggest that an update of the 1986 ECPA may be overdue.

6. Some Suggested Guidelines for Developing New Regulatory Policy

The most basic principles should govern the development of new policy.

- It should always be possible for the courts, for law enforcement, and for national security agencies to get data for which there is a valid need, and to obtain it in a timely fashion when necessary to prevent criminal acts or acts of terrorism.
- Demands for data should always be subject to appropriate review.

The first suggests that locating data where it cannot possibly be subject to search with a valid warrant cannot be tolerated — e.g., if a service provider locates data on an artificial island, or in a safe data haven not subject to any MLATs (*Mutual Legal Assistance Treaties*), then domestic law applies. Even here there is significant ambiguity. Whose domestic law should apply? The law of the country in which the service provider has its home office? The law of the country in which the service provider contracted with the customer? The law of the customer's home country? Likewise, the first principle suggests that encrypting data so that no one, not even the service provider, can access the data for any reason is a threat both to judicial proceedings and to national security. This suggests the need to address two separate but related concepts, *data citizenship* and *data sovereignty*.

Data citizenship refers to where the data are assumed to reside. When data are located in a specific location for reasons of performance, or to conform to national law about the retention of data relevant to a country's citizens, then that is the country of the data's citizenship. When data are located in no particular country and move around within the cloud, or when data are located in countries specifically to avoid surveillance, harmonized international standards need to be developed to determine whether the data has citizenship, or is in some sense stateless. Data sovereignty will be the rules governing which states have control over data that possesses its citizenship, and how to govern access to data that is in some sense stateless.

The second principle suggests that blanket warrants for data, without specifying the object of the search or the relevance of those objects to specific litigation, can only be used in the most restricted of cases.

The next section suggests policy, including some rules for harmonization.

7. Suggested Policy

There is a small set of actions that could easily be taken by all technology services companies and email providers. These actions would ensure that the outcome of a case would not be determined by delay caused by properly pursuing appropriate venues, simply by preserving potentially relevant evidence while warrants were pursued. Thus, no country would ever need to argue that in the absence of rapid search, including search of questionable legality, necessary email evidence would be lost forever. While this would not alter the need for speed in counter-terrorism operations, it would essentially nullify the arguments used by the Department of Justice in this case. The Congress should pass legislation that would make these actions mandatory for all service providers operating in the United States.

First, all email service providers around the world should be required to maintain backups of all email correspondence as soon as they receive a suitable official notification of an investigation anywhere in the world for which this email is material evidence and an official request for assistance in obtaining a valid search warrant. We are aware that backups are usually available, but this ensures that any email that was available at the time of notification would always remain available at the time the service provider received a valid warrant. This does *not* require the service providers to respond to a warrant from a foreign jurisdiction. It *does* require the service provider to maintain and protect archival data until such time as the case is resolved or the relevant jurisdiction where the data resides has issued a warrant. If such a valid warrant is issued, then and only then is the company is required to provide the data covered by the warrant.

Global harmonization is essential in regulating data services providers, just as it was in regulating securities trading, to avoid what well-regulated exchanges called *"the race to the bottom in securities regulation."* Regulatory harmonization in traditional industries likewise ensures that no country's manufacturers or service providers are placed at a disadvantage by adhering to stricter rules and so that no country's manufacturers or service providers gain a competitive advantage by being held to laxer rules. Thus, countries will not be able to compete through regulatory laxness. In the 1980s, during the early days of linked securities markets and global securities trading, there was considerable concern that competition among global trading centers would inevitably lead to competition to see which market could provide the least restrictive trading rules, often called competition through regulatory laxness and *"a race to the bottom"* [26]. If international norms in data privacy regulation are to be respected, then no nation should provide limited oversight simply for competitive advantage for its own service providers.

We need clear and unambiguous rules for establishing rules *data citizenship* and *data sovereignty*. Data citizenship tells us where the data resides for purposes of control, and data sovereignty tells us who determines what rights are allowed when accessing the data from anywhere in the world. Determining data citizenship will sometimes be straight-forward. When the service provider is located in the same jurisdiction as the data and as the data's owner, then unambiguously the data are presumed to have citizenship in that single country. Data citizenship is sometimes more complex. When the data and the data's owner are located in the same jurisdiction, but this is not the home location of the service provider, where should the data be presumed to have citizenship? By analogy with physical documents and physical search, we would assume that the data have citizenship in the country where they are stored. Any agent wishing to search the data would need to follow the rules of that country, again by analogy with physical search. If a German citizen stored documents in an office of an American bank located in Germany, a German warrant would be required for search, even though the data are located with an American firm. However, there will be occasions when, as a result of technical design or deliberate policies, data may appear to be *stateless,* as would occur if the data were stored in non-geosynchronous near-earth orbit, or more plausibly in a data center on an artificial island. Equivalently, the data might be deliberately stored in a data center in a rogue state with no MLATs. In this case the data might be treated as if it had the citizenship corresponding to the location of the service provider's home office, simply to ensure that no service provider maneuvered for competitive advantage by seeking to establish stateless data.

Data sovereignty tells us who is allowed to access data with an appropriate warrant. For data with clearly established citizenship, rights of data sovereignty are held by the country of the data's citizenship. The rights of sovereignty imply the application of that country's rules for search. MLATs can be negotiated. Additionally, given the ease with which cross border searches can be performed, countries may choose to extend the right of search to trusted allies, may choose to create expedited electronic MLATs (eMLATs), or may choose to leave traditional MLATs in place. When data are stateless, the rights of data sovereignty might be presumed to reside with the country where the service provider was located.

8. In Conclusion

Each of the four cases teaches us something different about privacy.

The Apple iPhone. The Apple iPhone dispute teaches us that there are indeed times when access to data may be urgently needed to avert an act of terrorism or other acts of mass violence. The devices of suspects may be searched with an appropriate warrant, and cooperation from hardware or software vendors should be compelled under these limited circumstances.

The Microsoft Email Warrant. Microsoft's dispute with the Department of Justice teaches us that whenever possible warrants for search of electronic documents should be consistent with the rules governing traditional search warrants. When data has foreign citizenship and a foreign country exercises legitimate data sovereignty, warrants should be obtained from the country with sovereignty.

The Google Email Warrant. Google's dispute with the FBI teaches us a lesson that is orthogonal to the lesson of the Microsoft case, but does not contradict it in any way. When documents are stored in such a way as to render them stateless, then international agreements and harmonized standards are required, if for no other reason than to preclude the tortured reasoning of the judge in this case. Regardless of what agreements are eventually reached, when the home country of the service provider with control of the data, the home country of the individuals who own the data, and the location of the alleged offense that justified issuing of the initial warrant are all the same, then the warrant should be considered valid and the search should be allowed to proceed.

The Facebook Warrant. Finally, the Facebook search warrant case teaches us that it is too easy to demand anything and everything with an electronic search, without establishing in advance what you are seeking to find. Warrants are not subpoenas and they cannot be contested or appealed to a higher court before complying. They have traditionally required specification of what is being searched, what is being sought, and why. This principle should be applied to warrants for the search of electronic media.

9. References

[1] Alderman, T. "Email Is Changing the Way We Communicate and Historians Are Worried", *The Huffington Post,* 25 May 2011, http://www.huffingtonpost.com/tom-alderman/email-is-changing-the-way_b_90050.html.

[2] Bravin, J. "Supreme Court: Police Need Warrants to Search Cellphone Data", *The Wall Street Journal*, 25 June 2014, https://www.wsj.com/articles/high-court-police-usually-need-warrants-for-cell-phone-data-1403706571.

[3] Cadwalladr, C. "Robert Mercer: the big data billionaire waging war on mainstream media", *The Guardian*, 26 February 2017, https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage.

[4] Clemons, E. K. "The Federal Government's Attempt to Force Microsoft to Violate Irish Territoriality — 'It's the wrong time, and the wrong place; Though your case is charming, it's the wrong case'", (Eric K. Clemons), *Proceedings, 50th International Conference on System Sciences*, Waikoloa, Hawaii, January 2017).

[5] Edelman, B. "Secret Ties in Google's 'Open' Android"", February 13, 2014, http://www.benedelman.org/news/021314-1.html.

[6] Edelman, B., and Luca, M. "Digital Discrimination: The Case of Airbnb.com." *Harvard Business School*, Working Paper, No. 14-054, (Jan. 2014).

[7] Edelman, B., Luca, M., and Svirsky, D. "Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment", (forthcoming) *American Economic Journal: Applied Economics*.

[8] "Electronic Communications Privacy Act", Wikipedia, 14 April 2017, https://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act.

[9] "Email Privacy", Wikipedia, 22 May 2017, https://en.wikipedia.org/wiki/Email_privacy.

[10] "Fairness Doctrine", Wikipedia, 8 June 2017, https://en.wikipedia.org/wiki/Fairness_Doctrine.

[11] "Federal Trade Commission", Wikipedia, 25 March 2017, https://en.wikipedia.org/wiki/Federal_Trade_Commission.

[12] "First Amendment to the United States Constitution", Wikipedia, 8 June 2017, https://en.wikipedia.org/wiki/First_Amendment_to_the_United_States_Constitution.

[13] "Food and Drug Administration", Wikipedia, 28 May 2017, https://en.wikipedia.org/wiki/Food_and_Drug_Administration.

[14] Goodman, M. "How technology makes us vulnerable", *CNN*, 29 July 2012, http://www.cnn.com/2012/07/29/opinion/goodman-ted-crime/index.html.

[15] Hatmaker, T. "Congress just voted to let internet providers sell your browsing history", *TechCrunch*, 28 March 2017, https://techcrunch.com/2017/03/28/house-vote-sj-34-isp-regulations-fcc/.

[16] Hovenkamp, H. Enterprise and American Law, 1936-1937, *Harvard University Press*, (1991) p. 154.

[17] Jan, T. "How racial bias could be hurting Silicon Valley's bottom line", *The Washington Post*, 24 February 2017, https://www.washingtonpost.com/news/wonk/wp/2017/02/24/how-racial-bias-could-be-hurting-silicon-valleys-bottom-line/?utm_term=.e09c93ba35ed.

[18] Johnson A. "Google CEO Backs Apple in FBI Fight Over Cracking San Bernardino Gunman's iPhone", *NBC News*, 18 February 2016, http://www.nbcnews.com/storyline/san-bernardino-shooting/google-ceo-backs-apple-fbi-fight-over-cracking-san-bernardino-n520421.

[19] Kerr, O. "2nd Circuit denies rehearing in Microsoft Ireland case by an evenly divided vote", *The Washington Post*, 24 January 2017, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/01/24/2nd-circuit-denies-rehearing-in-microsoft-ireland-case-by-an-evenly-divided-vote/?utm_term=.af533e7c700b].

[20] Kerr, O. "Google must turn over foreign-stored emails pursuant to a warrant, court rules", *The Washington Post,* 3 February 2017, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/03/google-must-turn-over-foreign-stored-e-mails-pursuant-to-a-warrant-court-rules/?utm_term=.d8d853e41cbb.

[21] Kiss, J. "Does privacy pose a threat to our private lives?", *The Guardian*, 21 August 2010, https://www.theguardian.com/technology/2010/aug/21/facebook-places-google.

[22] Kosinski, M. et al. "Mining Big Data to Extract Patterns and Predict Real-Life Outcomes", *Psychological Methods*, Vol. 21, No. 4, (Dec. 2016) pp. 493-506.

[23] Lichtblau, E. "Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman", *The New York Times,* 16 February 2016, https://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html?_r=0.

[24] Lichtblau, E., Benner, K. "Apple Fights Order to Unlock San Bernardino Gunman's iPhone", *The New York Times,* 17 February 2016, https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

[25] Lien, T. et al. "Apple CEO says helping FBI hack into terrorist's iPhone would be 'too dangerous'", *The Los Angeles Times*, 29 February 2016,

http://www.latimes.com/local/lanow/la-me-apple-san-bernardino-terror-20160218-story.html.
[26] Mahoney, P. C. "Securities Regulation By enforcement: An International Perspective", *Yale Journal on Regulation*, Vol. 7, No. 1, 7 (1990) p. 311.
[27] Markovikj, D. et al. "Mining Facebook Data for Predictive Personality Modeling", Association for the Advancement of Artificial Intelligence, Technical Report WS-13-01, (2013) pp. 23-26.
[28] McKinley Jr., J. C. "Facebook Loses Appeal to Block Bulk Search Warrants", *The New York Times,* 4 April 2017, https://www.nytimes.com/2017/04/04/nyregion/facebook-bulk-search-warrants-new-york-state.html?mcubz=1&_r=0.
[29] Mears, B. "Supreme Court: Police need warrant to search cell phones", *CNN,* 25 June 2014, http://www.cnn.com/2014/06/25/justice/supreme-court-cell-phones/.
[30] Miller, C. C. "When Algorithms Discriminate", *The New York Times*, 9 July 2015, https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html?_r=0.
[31] Nakashima, E. "FBI paid professional hackers one-time fee to crack San Bernardino iPhone", *The Washington Post*, 12 April 2016, https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.87abd513e9af.
[32] "Right to be forgotten", Wikipedia, 8 June 2017, https://en.wikipedia.org/wiki/Right_to_be_forgotten.
[33] *Riley v. California*, No. 13–132, reversed and remanded; No. 13–212, 728 F. 3d 1, affirmed (2014), https://www.law.cornell.edu/supremecourt/text/13-132.
[34] Ruane, K. A. Fairness Doctrine: History and Constitutional Issues, Congressional Research Service, Report No. R40009 (13 July 2011) p. 1.
[35] Shiller, B. R. "First-Degree Price Discrimination Using Big Data", Brandeis University, 19 January 2014.
[36] Tabuchi, H. "Yahoo Japan Teams With Google on Search", *The New York Times,* 27 July 2010, http://www.nytimes.com/2010/07/28/technology/28yahoo.html.
[37] Tett, G. "Donald Trump's campaign shifted odds by making big data personal", *Financial Times,* January 26, 2017, https://www.ft.com/content/bee3298c-e304-11e6-9645-c9357a75844a.
[38] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance. Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22.
[39] Wakabayashi, D., Maxwell, K. "Yahoo Japan, Google Ally", *The Wall Street Journal*, 27 July 2010, https://www.wsj.com/articles/SB10001424052748703977004575392412415127820.
[40] White, G. B. "When Algorithms Don't Account for Civil Rights", *The Atlantic*, 7 March 2017, https://www.theatlantic.com/business/archive/2017/03/facebook-ad-discrimination/518718/.
[41] Wu, T. *The Master Switch: The Rise and Fall of Information Empires*, Knopf (2010), pp. 384.
[42] Zalta, E. N. et al. Privacy and Information Technology, *Stanford Encyclopedia of Philosophy* (Spring 2016 Edition).