Privacy: An Issue of Priority

Stephanie Segovia

Follow this and additional works at: https://repository.uchastings.edu/hastings_business_law_journal

Part of the Business Organizations Law Commons

Recommended Citation
Available at: https://repository.uchastings.edu/hastings_business_law_journal/vol11/iss1/8
Privacy: An Issue of Priority

Stephanie Segovia*

I. INTRODUCTION

Privacy law in the U.S. has come under attack in recent years, especially within the context of online personal information. Data breaches of personal information are no longer an uncommon occurrence, and with the emergence of mass data gathering and “Big Data” technologies, average internet users have something to fear if they value their privacy. Phrases akin to “[P]rivacy is on its death bed,” or “Rethinking Privacy in an Era of Big Data” are becoming commonplace in the news. While the U.S. has been widely inactive in this area of the law, the European Union (“EU”) is taking aggressive steps towards enacting legislation intended to restore trust in the online world. Silicon Valley tech companies are up in arms in the aftermath of the EU directives, fearing the corporate impact of laws that require rigorous privacy protections for EU citizens. In contrast to the EU laws, the U.S.’s fractured data-breath system (which merely responds to violations instead of seeking to prevent them)

* Candidate for J.D., University of California, Hastings College of the Law, May 2015. The author thanks Professor Ben Depoorter for his valuable guidance and advice. The author also wishes to thank her friend Dustin Watson for his useful and insightful comments during the editorial process. Finally, the author thanks her family for their love and support in all of her endeavors.

2. Id.
3. See id.
seems to be a product of misaligned priorities because privacy is taking a backseat to corporate compliance costs. While privacy encroachments are becoming more common, the excitement of new data-gathering technology, coupled with only voluntary self-regulation, is initiating this snowball effect. The heavy lean towards alleviating corporate compliance costs is paving a wide and clear path for boundless technological innovation and, simultaneously, the degradation of online privacy in America. Privacy law in the U.S. not only needs to be rewritten, it is essential that it become a higher priority when measured against a business’s ability to comply with new comprehensive legislation. This paper argues that the EU’s new Privacy Directive (“Directive”) must be a guide for a comprehensive restructuring of privacy law in America. Specifically, the U.S. needs unifying legislation that can more appropriately deal with privacy encroachments than its current jurisdictional framework. Second, establishing a privacy commissioner in the U.S. will create a power source that can effectively advocate for individual privacy and facilitate a trusting relationship between the citizens and those that gather and use personal information. Third, the expansion of personal privacy definitions in the digital sense will further limit organizations from encroaching on an individual’s privacy. Finally, the indefinite coexistence of individual privacy and the tech industry will be realized by using the finances earned through privacy violations to fund research on how to alleviate corporate compliance costs through a set of procedures and incentives programs. Thus, priorities would be shifted away from over-emphasizing the reduction of compliance costs to making privacy controls a real and effective protection—a shift that users have a right to exercise and one that profitable organizations engaged in data collection can survive with comfort.

Part II of this paper highlights the competing stakes in the online privacy debate. It begins with a quick overview of the U.S. business model of companies that participate in data gathering and analysis, and why they do so (namely because of the emergence of Big Data
Part II concludes with some examples of how online privacy has eroded in recent years, in turn highlighting the need for federal action.

Part III discusses the current status quo of online privacy in America, and why current legislation is inadequate to address online privacy issues. This section then moves into a discussion of why the U.S. should let the new EU Directive be a guide for establishing its own comprehensive privacy protection framework, and concludes with an analysis of the most important principles that can be taken from the EU Directive. Additionally, strategies are discussed on how to incentivize companies to engage in beneficial research for the entire industry that could make the transition of complying with the new online privacy regulations more manageable.

It should also be noted that Facebook and Google are used in this note as examples in the “erosion of privacy” section. Both companies are metaphors for all companies engaging in activities that are likely to affect the privacy of online users. Facebook and Google are used because they are widely known and easy to relate to. However, I do not suggest that any of their privacy-infringing activities were intentional. The exploitation of personal data is how many businesses bring in revenue. Furthermore, the internet is constantly morphing into something new, and exploitation of individual privacy is likely to occur because this country has not yet defined what privacy means in the online context.

II. PRIVACY CONCERNS

A. THE U.S. BUSINESS MODEL

There are two important points to consider as background for understanding the erosion of online privacy:

(1) Companies like Facebook and Google offer services used by billions of users that have become central to the “average American’s” everyday life. Initially, Facebook was created to give

“people the power to share and make the world more open and connected.” The services are offered free to users, but free services imply that the user is in fact the product. Personal information is extremely valuable, and has become even more so with the dawn of “Big Data” technologies. Google and Facebook make a fortune collecting personal information to help them more accurately target their advertisement content. So far, the actions taken by these companies have not yet convinced regulatory authorities to legislate in this area. However, data-gathering sites and services continue to push forward with business models heavily geared towards the exploitation and acquisition of personal information. Thus, they should be forced to adhere to a more concise set of laws and regulations.

(2) Federal comprehensive legislation is needed to unify industry standards and protect consumers. Online users are at the mercy of companies like Facebook and Google that are operating under their own voluntary privacy policies (with the exception of federal regulation pertaining to health records and data about children younger than thirteen) without any real penalties because there are essentially no regulations for them to comply with.

Technological advancements act as crucial economic boosters for the U.S., but privacy will continue to suffer if its level of importance to Congress remains stagnant as this technological revolution empowers data-gathering companies to exploit online information in order to remain competitive.

13. Id.
B. THE EXCITEMENT OF BIG DATA

Big Data has been causing quite the stir in the global tech-world, and precisely what it means remains a mystery to the majority of the non-technical populace. Big Data is both structured and unstructured data generated from diverse sources in real time, in volumes too large for traditional technologies to capture, manage, and process in a timely manner. Big Data’s value depends on the organization’s ability to analyze it in useful ways. Thus, persons involved in analytics (relying on fields such as statistics, computer programming, and operations research) will be the key persons utilized to decode the information.

There is a flood of data created everyday by the interactions of billions of people using computers, GPS devices, cell phones, and medical devices. Online or mobile financial transactions, social media traffic, and GPS coordinates now generate over 2.5 quintillion bytes of so-called “Big Data” every day. This means the number 2.5 followed by eighteen zeros, which is the equivalent to 57.5 billion thirty-two GB iPads. The growth of mobile data traffic from subscribers in emerging markets is expected to exceed one-hundred percent annually through 2015. Researchers and policymakers are realizing the potential for channeling these torrents of data into actionable information that can be used to identify needs, provide services, and predict (or even prevent) crises before they occur.

Public health offers one of the most compelling areas where the

---

16. Id.
17. Id.
18. WORLD ECON. FORUM, supra note 14, at 1.
19. Id. at 2.
20. 2.5 Quintillion Bytes Created Each Day; Calculated Via West, STORAGE NEWSLETTER (July 26, 2012), http://www.storagenewsletter.com/rubriques/market-reports research/viawest-2-5-quintillion-bytes-each-day/.
22. Id. at 1.
analysis of internet data could lead to huge public gains. The San Francisco-based Global Viral Forecasting Initiative ("GVFI") performs data analysis on information mined from the internet to comprehensively identify the locations of outbreaks before they become global epidemics. GVFI's Chief Innovative Officer has stated that this technique can successfully predict outbreaks up to one week ahead of global bodies such as the World Health Organization that rely on traditional techniques and indicators.

Much of Big Data is primarily unstructured, and traditional databases cannot handle the vast quantity of this unstructured information. Thus, new technologies and new analysts who can use the technologies are necessary to make this information useful. The computer tools for gleaning knowledge from the internet's "vast trove of unstructured data are fast [and] gaining ground." At the forefront of these innovations are the rapidly advancing technologies of artificial intelligence like natural-language process, pattern recognition, and machine-learning. Machine-learning algorithms learn from data, and the more data, the more the machines learn. For example, take Siri, the talking, question-answering application in iPhones. When Siri was first introduced by Apple in 2010, she was helpful, but she often confused commands. Apple has been feeding her data since 2010, and now with people supplying millions of questions, Siri is becoming an increasingly adept personal assistant, and she rarely confuses the users' words anymore.

McKinsey Global Institute, the management consultancy's research arm, and the closest the corporate world comes to having an "ivory tower," published a 143-page report on Big Data in 2012. The report states that it was "the next frontier for innovation, competition, and productivity." McKinsey believes that Big Data

23. WORLD ECON. FORUM, supra note 14, at 5.
24. Id.
25. Id.
27. Id.
28. Id.
29. Id.
30. Id.
31. Id.
32. Chrystia Freeland, In Big Data, Potential for Big Division, INT'L HERALD TRIB., Jan.
will amount to a fifth wave of technological revolution, building upon the first four: (1) the mainframe era, (2) the PC era, (3) the internet and Web 1.0 era, and (4) most recently, the mobile and web 2.0 era.\(^3\)

Big Data could lead to a surge in productivity and the U.S. retail sector alone could increase a retailer’s operating margin by more than 60 percent.\(^4\) At the World Economic Forum in January 2012, in Davos, Switzerland, Big Data was the hot topic, and the report by the forum declared personal data “a new class of economic asset, like currency or gold.”\(^5\)

C. BRINGING BIG DATA INTO THE CONTEXT OF PRIVACY

Today, social-network research involves mining huge digital data sets of collective behavior data.\(^6\) Both Google and Facebook are “masters at harnessing the data of the web,”\(^7\) and their stake in this venture is large. The value of personal information and the progression of Big Data technologies will accelerate growth in the tech industry, and there is no doubt that online service providers (“OSPs”) (e.g., Google and Facebook) want to supply this information to the end-users in exchange for a profit.

The World Economic Forum report did more than praise the era of Big Data, it also flagged the obstacles with which a society could be confronted.\(^8\) “Data ecosystem actors” (OSPs that gather data, like Facebook and Google and the end-users who will purchase the data and analyze it) have much to gain from the creation of an “open data commons,”\(^9\) or more transparency. The report says, “[T]he sharing of such data especially that tied to individuals raises legitimate concerns that must be addressed to achieve the cross-sector collaboration . . . [C]oncerns about violating user trust, rights of expression, and confidentiality” will occur.\(^10\) Privacy concerns must be addressed

---

33. Freeland, supra note 32.
34. Id.
35. Lohr, supra note 10.
36. Id.
37. Id.
38. WORLD ECON. FORUM, supra note 14, at 5-6.
39. Id at 5.
40. Id.
before firms, governments, and individuals can be convinced to share data more openly.\textsuperscript{41} What is more interesting is that after an extensive Big Data subject analysis, the report concludes with a directive note that it will be necessary for governments around the world to play a role in setting the legal frameworks for governing data privacy and security.\textsuperscript{42} Legislative legal frameworks should be created that (1) protect the individual, and (2) require contractors to make their data public, thus honing in on the business value that data philanthropy can deliver.\textsuperscript{43} The World Economic Forum has recognized that new technologies falling under the banner of Big Data will certainly implicate individual privacy rights and that legislation will be necessary to alleviate this transition. More importantly, legislation will be key for encouraging consumers to share their information so that it can be analyzed because requiring more transparency will allow consumers to build trust in the OSP.

D. THE EROSION OF PRIVACY IN THE U.S.

Today, a ten-minute Google search can lead to someone’s phone number, home address, place of employment, life photos,\textsuperscript{44} or even a person’s morning run path through the use of an iPhone.\textsuperscript{45} Employers can discover someone’s general age (by looking at the date of a picture),\textsuperscript{46} his or her attractiveness, whether he or she played sports in college, et cetera. Location services can tell someone exactly where another person is currently standing anywhere on the Earth. Coupled with readily available online information, this ease can create a serious risk of harm to one’s reputation, limit one’s ability to control his or her own image,\textsuperscript{47} and ultimately, affect the individual’s happiness.

Privacy is on its deathbed in America, and while subtle privacy

\begin{itemize}
  \item[41.] World Econ. Forum, supra note 14, at 5.
  \item[42.] Id. at 7.
  \item[43.] Id.
  \item[44.] Bilton, supra note 1.
  \item[45.] Id.
  \item[46.] Id.
  \item[47.] Karen Majovski, Data Expiration, Let the User Decide: Proposed Legislation for Online User-Generated Content, 47 U.S.F. L. Rev. 807, 810 (2013).
\end{itemize}
invasions seem harmless to a generation thankful and eager to be a part of the technology age, U.S. citizens should consider their lack of privacy a serious issue since it has only been degrading and has never been strengthened. Elizabeth Stark, a lecturer at Stanford, highlights this point, “We used to have privacy through obscurity online, so even if people had that information out there, the steps that it would take to aggregate were all too great.” She goes on, “Previously you could have searched every photo of Nick Bilton until you eventually found one, but that would take a lifetime. Now, facial recognition software can return more images about someone instantly.” Obscurity is no longer an option for online users in an age where people have been uploading personal information to the internet for upwards of twenty years.

Facebook is one of the star players in this privacy debacle because of its data-gathering capabilities and its user network of over one billion individual contributors. Facebook enables users to communicate and receive personal information via Timeline posts viewable to a broader audience or through direct, one-on-one communications or messaging with another individual. In recent years, Facebook has been criticized by privacy advocates for (1) its obscure privacy settings, (2) its data-sharing with third-party advertisers, and (3) interception of seemingly private conversations or deleted materials.

Michael Zimmer, director of the Center for Information Policy Research at the University of Wisconsin-Milwaukee, has begun a project called the “Zuckerberg Files.” Zimmer, someone who has spent years challenging Facebook on privacy issues, is creating a digital archive of every word Zuckerberg has ever uttered. The point
is to track Zuckerberg’s evolving views of privacy, but Zuckerberg’s evolving views also represent the erosion of the idea of privacy in the online world as a whole. During Facebook’s birth, Zuckerberg said that Facebook’s success was dependent on people feeling comfortable sharing information on the social network. In 2009, Zuckerberg said, “Our philosophy is that people own their information and control who they share it with.” In 2006, Facebook created the “NewsFeed,” where people could update all of their friends by posting to the NewsFeed. Little did they know, the privacy settings were completely absent from the feature. When users began to voice concern, Zuckerberg responded with, “We really messed this one up.” In 2010, after another privacy restructure, Facebook left users so confused as to what they were sharing that many wound up sharing personal information with people they never intended to share with. For example, when a user tags his or her friend in a post or photo, the friend’s privacy settings apply instead of the user’s own privacy settings. Zuckerberg’s response was, “Many of you thought our controls were too complex . . . . Our intention was to give you lots of granular controls; but that may not have been what many of you wanted. We just missed the mark.” Today, Facebook’s privacy settings are still complicated and unreliable. Although users are given the option to control the privacy of some of their information, Facebook continuously revamps its privacy controls, making it difficult for users to stay informed about how privacy settings work for them.

Agnieszka McPeak, professor of law, published an extensive report of the inner workings of Facebook. Her research shows that a single Facebook account includes the data that the user uploads to the social media website, and information that Facebook compiles about the user as a result of the user’s interaction with different

54. Dwoskin, supra note 52.
55. Id.
56. Id.
57. Id.
58. Id.
59. Id.
60. McPeak, supra note 50, at 906.
61. Id. at 901.
applications. The latter, although based on user activity, extends beyond items the user intentionally made available to others. For example, the data stored by Facebook includes personal information the user deliberately shielded from others through their website’s privacy settings. This means that the “profile” Facebook creates about a user, and then later sells to advertisers, includes intentionally-shared information as well as deliberately shielded information. Facebook has faced litigation over its advertising practices and purported sharing of personal user information with advertisers. In December 2013, Facebook was sanctioned by the Federal Trade Commission (“FTC”) for not respecting the “privacy and wishes of its users,” through its Sponsored Stories feature. Facebook was forced to pay twenty million dollars in compensation, and is now subject to privacy audits for the next twenty years. Facebook, without warning its users or seeking consent, made public to third parties information that users had deemed private on their Facebook pages. Advertisers were allowed to obtain personally-identifiable information when Facebook users clicked on an advertisement displayed on the users’ Facebook pages. Facebook announced that it would ax the feature altogether in April 2014. Additionally, January of 2014 began with other privacy complications. Facebook was served with a class action lawsuit filed in the U.S. District Court for the Northern District of California, filed on December 30, 2013.

62. McPeak, supra note 50, at 907.
63. Id.
64. Id. at 910.
65. Sengupta, supra note 6.
66. The FTC is an independent agency of the U.S. established in 1914 by the Federal Trade Commission Act. Its mission is the promotion of consumer protection and the elimination and prevention of anticompetitive business practices.
69. Sengupta, supra note 6.
70. Id.
71. Id.
72. Faull, supra note 68.
complaint states that Facebook systematically scans users’ private messages and reads URLs shared through messages by intentionally intercepting electronic communications, adding that by doing so, the social networking giant has violated the Electronic Communications Privacy Act and California’s privacy laws. The complaint alleges that Facebook represents to users that the content of Facebook messages are “private,” which gives an impression that its free message service is free from surveillance, and that this misleading representation encouraged users to provide information through the message that they might not have shared if they knew that they were being intercepted. The practice is being done because it enables Facebook to mine user information (i.e., interests and desires) and profit from selling that information to third parties—namely, advertisers, marketers, and other data-aggregators (end-users) who will exploit the information. While Facebook is calling the allegations “without merit,” the plaintiffs cite third-party research to back up their claim.

Third-party end-users were allowed access to photos and videos even after a Facebook user had deleted her account. Facebook has not been forthcoming as to how it retains deleted data. What is known is that deleted items linger on Facebook servers for an indeterminate amount of time. Before 2012, Facebook took years to remove deleted photos from their servers, and anyone with the URL

---

74. VN, supra note 73.
75. Id.
76. Id.
77. Id. (Among the support for their claim is information gathered in August of 2013 by High-Tech Bridge, a Swiss security firm, which revealed that Facebook scanned user URLs in private messages. High-Tech Bridge conducted a study of the fifty largest social networks, web services, and free email systems, and created a dedicated web server and generated a secret URL for each online service. The researchers then used the private messaging function of each web-based service to embed a unique URL in each message, and monitored its servers’ weblog to see whether any of the services (Facebook) would “click” on the dummy URLs that had been transmitted via private message. And according to the findings, Facebook was one of the web-based services that scanned URLs in private messages without disclosing such activity to its users).
78. End-users are those that use the personal information provided to them by OSPs.
79. Sengupta, supra note 6.
80. McPeak, supra note 50, at 905.
81. Id.
of a deleted photo could still access the photo using the URL (highlighting the individual’s lack of control over their private information). The new system is said to delete photos from servers within one month of deletion by the user. Still, it takes an act of Facebook to actually delete the content from its servers.

Silicon Valley tech giant Google is the other obvious player in the information privacy debate. In early January 2014, it announced a “Shared Endorsement” feature—similar to Facebook’s Sponsored Stories—that will utilize users’ names and profile pictures in advertisements. Through endorsements, Google will display your reviews, recommendations, and other relevant activity throughout its products and services. Users can “opt out” of this feature in their account settings. Still, social media default settings generally favor openness at the expense of personal privacy, and users are often unaware of how to navigate the settings. The process of opting out is unclear and Google signs its users up for its features automatically, leaving people like Kristen Burnham, Senior Editor for InformationWeek, to write an entire article on how to opt out of features like the Shared Endorsements. Immediately following the endorsement feature, Google was cited by Canada’s Privacy Commissioner, who stated that Google violated the country’s privacy laws after it used a person’s internet searches about a personal health

82. McPeak, supra note 50, at 905.
83. Id.
84. Id. See also Alessandro Acquisti & Ralph Gross, Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, in PRIVACY ENHANCING TECHNOLOGIES 36–58 (George Danezis & Philippe Golle eds., 2006), available at http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf (explaining how Facebook’s access controls are weak by design, and that information will exist as long as anybody has an incentive to maintain it).
86. Id.
matter to tailor advertisements he would see when surfing online.\textsuperscript{89} The Canadian resident searched how to best treat his sleep apnea and later, on completely unrelated websites, the complainant would see ads highlighting devices to help apnea sufferers breathe.\textsuperscript{90} The Commissioner said Canada’s guidelines on behavior advertising forbid advertisers from collecting sensitive personal information, such as individuals’ health information, for the purpose of delivering tailored pitches, and that its privacy laws mandate an individual’s explicit consent for the collection and use of personal information.\textsuperscript{91} It further scolded Google by stating that “implied consent” for the collection of personal health information is “not appropriate.”\textsuperscript{92} A user should be able to search embarrassing symptoms without fearing this information will be exposed in any manner or form. If Google’s shared endorsement feature even remotely connects the user’s illness with him on his own computer or to other Google+ members, he is likely to be discouraged from researching anything controversial on Google at all, thus shutting off an extremely important avenue of health information for the internet user.

The above examples represent some effects of self-regulation and how a lack of comprehensive guidelines in the online businesses environment contributes to the erosion of privacy in the U.S.

III. U.S. INFORMATIONAL PRIVACY LAW

A. U.S. PRIVACY LAW AND THE KATZ STANDARD

The protection of privacy in the U.S. is derived from the Fourth Amendment of the United States Constitution. The 1967 case, \textit{Katz v. United States}, provides the current standard for assessing whether someone’s expectation of privacy has been violated, or when the government should take measures to protect against a privacy encroachment.\textsuperscript{93} That standard is as follows: (1) A person must have a subjective expectation of privacy, and (2) that expectation is one that

\textsuperscript{89} Viera, \textit{supra} note 6.
\textsuperscript{90} Id.
\textsuperscript{91} Id.
\textsuperscript{92} Id.
\textsuperscript{93} \textit{See generally} Katz v. United States, 389 U.S. 347 (1967).
society is prepared to recognize as reasonable. 94 It is argued that disclosure of private information to third parties by companies like Facebook undermines an argument that the information should still be protected (third party disclosure rule). 95

Online privacy plaintiffs in the social media context generally fail in U.S. courts because of the following argument. (1) Social media websites are not private. They exist for the purpose of facilitating social behavior between individuals, and they are not intended to serve as personal journals shielded from others or a database for storage. 96 (2) Under a simplistic definition of privacy, nothing on social media websites can ever be protected as “private” by the very nature of this medium. 97 It is not reasonable to expect privacy protections when an individual voluntarily discloses her personal information to third parties. (3) Therefore, any expectation of privacy that one has concerning the exploitation of his or her personal information, whether on Facebook or Google or any other data-gathering website, is not one that “society is prepared to recognize as ‘reasonable.’” 98 However, the nature of the “medium” is exactly why privacy protections should be beefed up. That social media websites have “privacy” settings is what attracts people to the sites, making them feel comfortable uploading information that conveys their personal life to the online world. Users join Facebook or use Google’s search engine with the expectation that they have the power to (at least to some degree) control the exploitation of their information. When Facebook began in 2004, the platform was simplistic and privacy was not an issue because of Facebook’s minimal functionality. At that time, Facebook was not incentivized to gather information about its users and, directly or indirectly, invade their privacy. Today, Facebook and its users exist in a different world. Thus, the U.S. is in a different posture with regards to online privacy than it was ten years ago when data-gathering was not as efficient or exploitable.

96. McPeak, supra note 50, at 929.
97. Id.
The U.S. Supreme Court Justices have begun to foreshadow that the *Katz* test may be affected by the advancements of technology. 99 In the recent 2012 case, *State v. Jones*, Justice Alito (with whom Justices Ginsburg, Breyer, and Kagan joined in concurrence) spoke of the *Katz* standard in the context of technological advancements:

[T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the trade off worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable. 100

Justice Sotomayor says that it “may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties” because this approach is “ill suited to the digital age, in which people reveal a great deal of information about themselves . . . in the course of carrying out mundane tasks.” 101 She takes note of Alito’s point that some people may find the trade-off “worthwhile,” but she says that phone numbers, e-mail addresses that correspond with internet services providers, books, groceries, and medications purchased from online retailers, are a few examples of lists she would not want disseminated without her explicit permission. 102 While she notes that online society’s expectations of online privacy could only attain constitutional protection if Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy, she also clearly states that she does not believe that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason

---

101. *Id.* at 957 (Sotomayor, J., concurring).
102. *Id.*
alone, disentitled to Fourth Amendment protection.\textsuperscript{103} Even in 1967, Katz stated that “[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”\textsuperscript{104} Therefore, in light of new technologies, even the Supreme Court Justices are reevaluating the proposition that any disclosure of personal information to third parties outright defeats a reasonable expectation of privacy argument for one who makes available information to an OSP in exchange for use of the online product. According to Justice Alito, the real question should be: Does Facebook or Google’s use of online personal information rise to a degree of intrusion that a reasonable online user would not have anticipated?\textsuperscript{105} It strains reason to say that online users are completely aware of how their information is being used, or that they will consent to how it will be used in the future. For example, New York Times writer Steve Lohr offers the following example of a situation that, he and others believe, is not far into the future: imagine someone is looking for a gift for a friend and he or she is searching for a deep fat fryer. The data miner, tracking the user’s every click stream, records this information and makes a data-based prediction that the user lives an unhealthy lifestyle. This information (in the form of a prediction) is then purchased by the user’s health insurer, and the user’s premiums rise.\textsuperscript{106} This is an example of a use of a consumer’s personal data that he or she would not reasonably have anticipated. Therefore, the U.S. test for privacy deriving from the Katz case should be reevaluated and, when it is, data-gathering techniques and their uses will have to be considered to determine what a reasonable expectation of privacy is in an age of Big Data analysis.

Although online privacy tensions are in a state of stress, Justice Alito says this could be exactly what is needed to spur legislation in the area of online privacy. He writes, “In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.”\textsuperscript{107}

\textsuperscript{103} Jones, 132 S. Ct. at 957.
\textsuperscript{104} Katz, 389 U.S. at 351.
\textsuperscript{105} See Jones, 132 S. Ct. at 964 (Alito, J., concurring).
\textsuperscript{106} Steve Lohr, Big Data Is Opening Doors, but Maybe Too Many, N.Y. Times, Mar. 24, 2013, at BU3.
\textsuperscript{107} Jones, 132 S. Ct at 964 (Alito, J., concurring).
B. LEGISLATION IN THE U.S.

So far, online privacy has not been deemed sufficiently worthy of protection in the U.S. and, therefore, Congress has done little to protect it. However, as noted in the opinions above by Justices Alito and Sotomayor, the fruition of new privacy concerns has arrived with new technologies, and consumers should not have to choose between new technology and privacy.\textsuperscript{108} The Electronic Communications Privacy Act ("ECPA") of 1986\textsuperscript{109} is the law that protects an individual’s electronic life (email, cell phone location records, Facebook posts, search history, cloud-computing documents). The ECPA was passed twenty-seven years ago.\textsuperscript{110} The outdated ECPA allows the government to intercept and access a treasure trove of information about “who you are, where you go, and what you do, which is being collected by cell phone providers, search engines, social networking sites, and other websites every day.”\textsuperscript{111} In no way at all was the Act intended to be a guideline for the States to protect online privacy. In fact, it would not be ridiculous to say that online privacy took a big hit when companies that can easily gather personal information, like Facebook, began popping up.\textsuperscript{112} Online privacy issues that arise today were nonexistent in the 1980s and the 1990s, and electronic surveillance legislation (the purpose for the Act) was not intended to preempt state law.\textsuperscript{113} States were encouraged to devise their own statutory schemes for electronic surveillance.\textsuperscript{114} Statutory schemes developed and produced a patchy and inconsistent framework throughout the U.S.

There are fundamental differences between the sectorial approach to information privacy adopted by the U.S. and the comprehensive approach to data protection adopted by the EU.\textsuperscript{115}
U.S. privacy law is characterized as “data-breach” notification law because it responds to incidents that have already occurred. The purpose of data-breach notification law is directly linked to identity theft. A majority of state-based laws are based on California’s data-breach system, which requires businesses to notify California residents of an existing or potential data breach that includes the unauthorized acquisition of unencrypted and computerized personal information. Data-breach systems have two conceptual aims: (1) The underlying principle that an individual has a “right to know” about unauthorized misuse of his or her personal information, and (2) the system encourages organizations to adopt better security practices. Safe harbors for companies allegedly encourage a wider adoption of encryption technologies for the storage and use of personal information. However, these reactionary (rather than preemptive) goals of the U.S. data-breach system make it easier for companies to avoid regulation because there is essentially no regulation to comply with. Minimal protections (e.g., a “right to know” of violations) are provided only after an adverse event has already occurred, and companies are not required to meet preventative goals that ensure adverse events do not occur in the first place. The examples provided above in Section II.D. show that self-regulation has not prevented companies from invading the privacy of their consumers. Thus, in the U.S., it is clear that corporate compliance costs are prioritized over the privacy interest of the average online user.

C. THE NEW EU DIRECTIVE ON NETWORK AND INFORMATION SECURITY

In contrast to the U.S. approach, the EU has developed a comprehensive approach to data protection. This framework
establishes information privacy rights for individuals and defines obligations for data-collecting organizations regardless of industrial sector (unlike the U.S. approach). In regards to individual privacy, the superiority of EU’s laws can be shown with an examination of its new Directive on Network and Information Security (the “Directive”) that, if enacted, will create the world’s toughest regulations governing data collection, use, and protection in the world’s largest economy.

The EU legislation’s goal of “creating trust” distinguishes it from the laws of the U.S. from the outset. The impending EU law contains ninety articles regulating data privacy protection, based on the proposition that control of an individual’s personal data is a fundamental human right, and includes the right to consent, the right to access, and the right to be forgotten. Paul Nemitz, European Commission director of fundamental rights and citizenship, told a packed theatre in Brussels at the International Association of Privacy Professionals Conference in December 2013, “I believe privacy will become a competitive advantage for European companies... There are millions of U.S. and Chinese middle-class consumers who do not want to be constantly tracked and analyzed without knowing what happens to their data and their money” (recall the deep fryer example). Vice President of the European Commission, Viviane Reding, writes that the lack of trust between citizens and data-gathering companies is highly damaging to citizens’ faith in the rule of law. It is also damaging to economic growth when citizens do not trust businesses with their private information. Reding warns that those companies who ignore people’s concerns are putting a lot more at stake than they realize. The proposed legislation is the EU’s attempt to avoid the complete loss of trust in companies engaged in

---

121. Burdon, supra note 115, at 85.
122. Lucas, supra note 4.
123. Id.
124. Id.
125. Id.
127. Id.
128. Id.
online business, and it is expected to become law in 2015.\footnote{129}

The new measures would prohibit the use of a range of standard Web tracking and profiling practices that companies currently use to produce targeted advertising, unless the get consumers’ explicit, prior consent.\footnote{130} The bill would also grant European consumers a fundamental new right: data portability, or the right to easily transfer an individual’s posts, photographs, and videos from one online service site to another.\footnote{131} Although negotiations are not complete, there are some key provisions upon which the Parliament and the Commission seem to agree. (1) Expansion of the definition of “personal data.” Personal data would be defined as any information relating to an individual, whether it relates to his or her private, professional, or public life.\footnote{132} It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, or a computer’s IP address.\footnote{133} (2) Data controllers (e.g., any company that collects personal information) would be required to obtain (and not assume) the express consent of the data subject to the processing of his or her personal data for one or more specific purposes.\footnote{134} The individual may withdraw the consent at any time, and consent is not valid where there is an “imbalance” between the position of the individual and the business.\footnote{135} Implicit in this is that opt-out options will not be sufficient,\footnote{136} making it more likely the user will have the chance to understand the privacy setting. (3) Businesses must adopt policies and implement appropriate measures to ensure and be able to demonstrate that their processing of personal data is performed in compliance with the Directive, including maintaining documentation


\footnote{131} Id.


\footnote{133} Id.

\footnote{134} Id.

\footnote{135} Id.

\footnote{136} Id.

\footnote{137} Lucas, supra note 4.
of processing activity.\textsuperscript{138} The key principle here is encouraging a high level of transparency so that data subjects will know what data is to be collected, by whom it will be collected, and how and where it will be used or stored.\textsuperscript{139} (4) Businesses with more than 250 employees are required to appoint a data protection officer responsible for monitoring data processing activities.\textsuperscript{140} The same rules apply to small companies who process the data of more than five thousand individuals.\textsuperscript{141} (5) International companies with European customers would have to comply with the directive’s regulations or face fines totaling two to five percent of their global revenues, or $138 million, whichever is greater.\textsuperscript{142} These are just a few provisions of the very extensive effort being put forward into creating this comprehensive framework that holds data gatherers accountable for infringements on an individual’s privacy.

The key aspect of this Directive is that it is based on the idea that privacy rights should not be disintegrated merely because the context is the internet. Neelie Kroes, the Vice-President of the European Commission responsible for the Digital Agenda, issued a speech on February 28, 2014, in Brussels. She made her position very clear: these are not digital rights, nor online rights; they are fundamental rights to privacy, and they apply just as much online as off.\textsuperscript{143} According to Kroes, the EU must put its foot down to provide protections for its citizens based on transparency, responsibility, and accountability.\textsuperscript{144} She noted that privacy protections are also about the “simple things,” such as people trusting that their personal data on social networks is protected.\textsuperscript{145} “Without security, there is no privacy; nor true freedom.”\textsuperscript{146} The EU is aware that organizations will have to restructure their business models to comply with the new standards. However, the ambitious nature of the new legislation is

\textsuperscript{138} Foster, supra note 132.
\textsuperscript{139} Id.
\textsuperscript{140} Id.
\textsuperscript{141} Id.
\textsuperscript{142} Scott, supra note 129.
\textsuperscript{143} Neelie Kroes, Vice-President, Eur. Comm’n for Digital Agenda, A secure online network for Europe, Address at Cyber Security Conference in Brussels (Feb. 28, 2014).
\textsuperscript{144} Id.
\textsuperscript{145} Id.
\textsuperscript{146} Id.
seen as the only way to make the legislation actually effective.\textsuperscript{147} The EU seeks to make it financially inefficient for organizations to brush off the Directive by paying insubstantial fines. If the legislation is passed and it does not make the “necessary improvements,” it is likely to weaken businesses and the EU’s economy.

The Directive is not meant to anchor privacy rights at the expense of data-gathering enterprises, and neither should the U.S. in its attempt to legislate. Rather, it recognizes that this is just the beginning of new technological possibilities and there seems to be no slowing down. At the same time, it is clear that privacy rights are disintegrating. Thus, the legislation is a way of disallowing the disintegration of privacy rights, reversing some of what individuals have lost in regards to information privacy, and bracing for the future and new advancements. As Kroes stated, “We have the technological ability to do immense, unprecedented things. Many of those things are positive; some are damaging, and increasing reliance [on OSPs] means increasing vulnerability [for individuals].”\textsuperscript{148} The EU recognizes that there is going to be a steep public interest trade-off for companies who are going to be making billions of dollars from new technologies,\textsuperscript{149} and this “data protection” should not be viewed as “data protectionism.”\textsuperscript{150} She wants EU citizens to see security as pivotal to their business models and central to competitiveness. In no way does Kroes deny that the EU wants to take advantage of the “huge boost of big data, and the benefits of this open innovative, unified global network.”\textsuperscript{151}

Another feature that distinguishes the Directive from U.S. privacy law is that while recognizing the benefits of investing in Big Data technology, it also recognizes that privacy is headed down an uncharted path. The darker side of the issue is difficult to pinpoint as there is little transparency in an unregulated industry. Danah Boyd, a senior researcher at Microsoft Research, stated, “Privacy is a source of tremendous tension and anxiety in Big Data . . . It’s a general

\textsuperscript{147} Kroes, \textit{supra} note 143.  
\textsuperscript{148} \textit{Id}.  
\textsuperscript{149} Lucas, \textit{supra} note 4.  
\textsuperscript{150} Kroes, \textit{supra} note 143.  
\textsuperscript{151} \textit{Id}.  

Winter 2015  PRIVACY: AN ISSUE OF PRIORITY  215
anxiety that you can’t pinpoint, this odd moment of creepiness.”\textsuperscript{152} In addition, an \textit{Economist} article comments on Julia Angwin’s discoveries through her oversight of a pioneering series of \textit{Wall Street Journal} articles titled “What they Know,” starting in 2010.\textsuperscript{153} The article provides some of Angwin’s real world examples of where the privacy discussion is headed: (1) A company that runs a fleet of camera-equipped cars that scan the number plates of one million vehicles a month to find those wanted for repossession, and then sells this data to insurers or private investigations, and (2) Angwin gets a credit card using an alias; she uses an anonymous search engine and encrypts her e-mail and texts; she leaves LinkedIn (a professional networking site).\textsuperscript{154} When she turns off basic web-browsing functions that enable tracking (called “cookies”), she becomes digitally paralyzed. Amazon items appear to be out of stock and she is unable to set up an appointment at an Apple store.\textsuperscript{155} The article concludes that the real story about the economy of personal information and protecting privacy in an age of Big Data has yet to be written.\textsuperscript{156} As Boyd iterates, “Regulation is coming . . . Technologies need to re-engage with regulators [and] get a model where we really understand usage.”\textsuperscript{157}

D. A TIME FOR LEGISLATIVE ACTION IN THE U.S.

The U.S. privacy regime must be rewritten, and the EU Directive provides strong starting points for new online protections. There are four key principles that the U.S. should be conscious of when drafting new legislation.

1. \textit{Unifying Legislation Is Needed}

The EU provisions are meant to replace the “hodgepodge” of privacy rules across the 28 EU member states with a single body of

\textsuperscript{152} Hardy, supra note 1.
\textsuperscript{153} Watching the Watchers, supra note 11.
\textsuperscript{154} Id.
\textsuperscript{155} Id.
\textsuperscript{156} Id.
\textsuperscript{157} Hardy, supra note 1.
law, giving business and citizens greater certainty about their rights and responsibilities. Similarly, the U.S. needs a comprehensive framework that provides more predictability rather than having the states legislate inconsistently on issues that affect all citizens. Self-regulation is plainly not working. Proponents of legislation argued that the industry is a “Wild West” where consumer data is gathered and sold without restriction. Currently, the states define their own privacy frameworks and have differing definitions of important key terms. The Electronic Frontier Foundation said, “Congress should feel pressure to update the law to protect everyone across the country. Now that states as politically diverse as California, Texas, and Maine are taking affirmative steps [to update privacy issues concerning sensitive electronic data], Congress should see that privacy legislation is bipartisan and feasible.” Peter Fleischer, Google’s top privacy lawyer, stated on his personal blog in 2014, that he is hopeful that the EU’s lawmakers will write “a better, more modern and more balanced law.” An editorial in the New York Times has stated that efforts to improve protection are not advancing in Washington. For example, in 2010, the FTC made little progress with its “do not track” proposal that would give users an easy way to prevent companies from amassing information about them to pitch ads. Even in the context of solely technology and marketing companies, the Obama administration continues to stand by voluntary industry standards. However, the best way to ensure that

161. Id.
164. Id.
165. Id.
Americans can protect their online personal information is through federal legislation backed by regulatory enforcement.\textsuperscript{166}

2. The U.S. Needs a Regulatory Enforcer Specifically Dedicated to Online Privacy

Kroes, mentioned in Section II.C above, is the Vice-President of the European Commission responsible for the Digital Agenda. Canada has a privacy commissioner.\textsuperscript{167} Why does the U.S. not have any comparable entity? In fact, the recent crackdowns on Facebook and Google (which created more transparency for U.S. citizens) were led by Canada, the U.K., and other countries with stronger privacy laws.\textsuperscript{168} Privacy commissioners are extremely valuable because they have extensive experience with administering fair information practices under national laws, are institutionally imbued with those of personal privacy protection, understand its technological implications, and are sensitive to inter-jurisdictional differences.\textsuperscript{169} They serve as international emissaries of data protection principles and the rights of individuals.\textsuperscript{170} A privacy commissioner would also be able to dedicate more specific attention to technological infrastructures to make regulation more compatible with the tech-industry.

In the U.S., internet privacy issues are policed by the FTC, which can take action only if a privacy-violating action is deemed “deceptive” or “unfair.”\textsuperscript{171} In 2010, there were talks that the U.S. may obtain a privacy commissioner and that privacy advocates would be reluctant to back any legislation lacking enforcement because it would be perceived as “toothless,”\textsuperscript{172} but that did not happen. Establishing a privacy commissioner would be a huge leap for online privacy improvements because for the first time in the U.S., there would be a powerful entity whose sole priority is to protect the

\textsuperscript{166} Editorial, supra note 163.

\textsuperscript{167} Vieira, supra note 6.

\textsuperscript{168} Angwin, supra note 159.


\textsuperscript{170} Id.

\textsuperscript{171} Id.

\textsuperscript{172} Id.
privacy of individuals. Canada’s privacy commissioner takes a back seat to no one.\textsuperscript{173} He is incredibly active and has criticized the U.S. for its lack of attention to privacy.\textsuperscript{174} The Commissioner acts not only as administrator of Canada’s Privacy Act, but as a privacy advocate, privacy lobbyist, and privacy educator.\textsuperscript{175} He continuously asserts that privacy is imperiled and asks for additional powers.\textsuperscript{176} About fifteen years ago, the Canadian Commissioner requested that it be given the job of representing all persons in Canada who believe their privacy rights have been injured and the power to limit any activities by government and businesses it views to be incompatible with privacy protection for Canadians.\textsuperscript{177} That privacy advocates and other commentators have become so engaged in the online privacy debate is a sign that a privacy commissioner is needed—there is no one guarding against privacy encroachments and, therefore, the topic is being heavily engaged by academic scholarship. U.S. citizens deserve the kind of zealous advocacy that Canadian and European citizens are receiving.

3. The Expansion of the Definition of “Personal Data” is an Important Update

The states have differing definitions of personal information, but most frameworks parallel California’s privacy regime.\textsuperscript{178} California uses the term “personal information,” referring solely to (1) Social Security number, (2) driver’s license number or California Identification Card number, and (3) the account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.\textsuperscript{179} Therefore, California is solely concerned with combinations of personal information that can be used to give rise to

\textsuperscript{\(174\)} Id.
\textsuperscript{\(175\)} Id.
\textsuperscript{\(176\)} Id.
\textsuperscript{\(177\)} Id.
\textsuperscript{\(178\)} Burdon, supra note 115, at 76.
\textsuperscript{\(179\)} Id. at 107.
identity theft harms.\textsuperscript{180} This mechanical approach does not compare to the EU’s approach, which encompasses “any information relating to an individual.”\textsuperscript{181} By expanding the definition of what kind of data will be regulated, new legislation will have a more meaningful impact because any new rules will not be limited to those companies that collect personal data. Rather, it will include entities like data processors—including cloud providers—because these companies also present an avenue for those who want access to data.\textsuperscript{182} Also, a broad definition avoids a context-specific or industry-specific approach. Since the right to privacy should be viewed as fundamental under a new legislative effort, there should be no reason to differentiate where encroachments should be more permissible. Individuals should know what kind of protections they have as citizens, not only as online users. In order to have that kind of predictability, an expansive definition of personal information, that includes any and all personal information will be necessary.

4. Most Importantly, Any New Legislation Must Impose Substantial Fines Imposed for Violations

Under the EU Directive, a company that willfully violates a privacy provision is subject to stiff fines.\textsuperscript{183} Giants like Facebook, Google, or Apple could potentially face fines of up to one hundred million Euros, or $140 million—five percent of their global turnover.\textsuperscript{184} The European measures would give governing bodies the right to impose fines in cases where a company violated privacy provisions, unlike the FTC’s power to impose fines only in cases where companies were found to have misled consumers about their data collection practices.\textsuperscript{185} As a response to these proposed measures, all major American tech companies have directed their lobbyists in Brussels, where the Parliament is based, to try and

\textsuperscript{180} Burdon, supra note 115, at 107.
\textsuperscript{181} Foster, supra note 132.
\textsuperscript{182} Reding, supra note 126.
\textsuperscript{183} Jolly, supra note 158.
\textsuperscript{184} Id.
\textsuperscript{185} Id.
weaken, or even remove, the Directive.\textsuperscript{186} Similarly, President Obama thinks the sweeping new privacy controls could hurt the U.S. tech industry in Europe.\textsuperscript{187} This is likely because the tech giants generate a third or more of those companies’ sales in the EU.\textsuperscript{188} Obama has stressed that the data-driven marketing economy provided $156 billion in revenue to the U.S. economy in 2012 alone.\textsuperscript{189}

The tech industry is not one that is lacking in financial stability, and those organizations will be able to handle a comprehensive restructuring of their compliance departments. Most of the tech giants are worth upwards of $150 billion.\textsuperscript{190} The smaller companies should also be able to handle restructuring their compliance departments because it will be on a smaller scale. Those companies that cannot comply with the regulations will be forced to find a means to do so or let the market evaporate their business. The U.S. economy does not offer unfettered prosperity; it offers a great breeding ground, with flexible start-up regulations, to enable small businesses to get on their feet. Still, new legislation and regulation is always a possibility in any society. The fines are even more justified when one considers the impossibility of putting a price on an individual’s right to control his or her own privacy.

Violators should pay fines, and those fines should fund technological research that can help facilitate corporate compliance problems with any new legislation. The idea that a bad actor can pay for technological research in its industry so that it may no longer be considered a bad actor is not a novel idea to the law. \textit{Boomer v. Atlantic Cement} is a widely known 1970 case that is likely taught in all law school courses that touch on the study of nuisance.\textsuperscript{191} In that case, a cement factory was deemed a nuisance because of the dirt,
smoke, and vibrations emanating from the plant that interfered with health and everyday lives of the neighboring landowners.\textsuperscript{192} These irritabilities interfered with the enjoyment of their property. Instead of halting the operations of the cement factory after the plaintiff (landowners) successfully proved their case, the court delivered a unique remedy. It recognized that the polluters were engaged in a lawful and necessary business, i.e., the creation of cement.\textsuperscript{193} The crucial point is that the solution to the problem was far from discovery at that time, and adequate technology procedures were yet to be developed that were economically practical.\textsuperscript{194} In fact, amelioration of air pollution would plainly depend on technical research in great depth and with great expenditure.\textsuperscript{195} Therefore, the highest court of New York decided that the factory would be subject to pay substantial damages for its pollution, thus incentivizing the industry to engage in research that could ameliorate their dilemma.\textsuperscript{196} This is the theory upon which the justification for the violations will rest. The online consumers are akin to the neighbors; they are persons who, in some way benefit from the tech industry, but who also do not deserve to be harmed by them. Violators will pay damages (fines) for their wrongful conduct, incentivizing them to engage in tech research that will allow them to comply with the regulations more efficiently.

The money obtained by the government or new privacy commissioner should then be used to fund non-violators’ research. Thus, both the violators and the nonviolators are incentivized to experiment with new technologies that could aid the industry in complying with regulations. The only difference is that the nonviolators will receive extra aid, while the violators must fund themselves, or at least they must do so until they become eligible again for funding.

The privacy commissioner should have wide discretion to incentivize the funding of research in creative ways. For example, the Republic of Cyprus is lagging behind other EU countries in

\textsuperscript{192} Boomer, 26 N.Y.2d at 222.
\textsuperscript{193} See id.
\textsuperscript{194} Id. at 222.
\textsuperscript{195} Id. at 223.
\textsuperscript{196} Id. at 225.
innovation. Nonetheless, the Cyprus Employers and Industrialists Federation established the “Cyprus Innovation Award,” which aims at the improvement of competitiveness of the Cypriot companies and increasing awareness of the importance of innovation. The deciding committee looks to things such as, “ways by which innovation has created competitive advantage in your business/organization/service,” and “changes which have occurred in the functionality of your business/organization/service [which] effect the innovation [and] the financial conditions (profitability, saving of resources, increase of productivity, etc.) within the organization.”

A U.S. privacy commissioner could construct a similar system that recognizes companies who make serious efforts to innovate in the area of privacy respectful data gathering. These awards could help guarantee that a particular company is not only successful, but that it is also committed to the protection of online privacy, creating more transparency and gaining more trust from its customer.

IV. CONCLUSION

Europe has historically been more protective of personal information than the U.S., while the U.S. has provided a breeding ground for entrepreneurs to innovate and for small businesses to prosper. There is no doubt that the tech industry has provided prosperity to the American economy and this should continue. However, what is occurring under the banner of Big Data technologies is extremely rapid technological growth, and this should not come at the expense of privacy protections. The lawsuits that Google and Facebook are dealing with are the beginning of many lawsuits that will follow as privacy encroachments continue to get worse and as new technologies makes it more economically efficient for organizations to exploit online personal information. Therefore, it is time for Congress to take federal preventive measures.

198. Id.
199. Id.
The EU Directive provides drastic, but strong, regulations to protect EU citizens and U.S. citizens deserve parallel protections. Congress needs to unify privacy law to avoid the splintered framework that is developing currently throughout the various jurisdictions. Furthermore, it needs to establish a privacy commissioner so that there is an empowered entity that focuses solely on the relationship between organizations involved in any kind of data gathering and the individuals who provide them with data. The commissioner will help facilitate the legislative transition into a privacy framework that does not prioritize corporate compliance over individual privacy, but puts individual privacy on an equal, if not higher, ground than corporate compliance costs. The corporations will have ample opportunity to engage in meaningful research to help their businesses continue to grow because: (1) they will be incentivized to do so for fear of paying large fines if they do not develop ways to comply with the regulations; (2) it will be desirable for them to develop technologies early on so that they are not fined, and can take advantage of financial support; and (3) lastly, it will be economically beneficial for the companies to receive something similar to the Cyprus Innovation Award because it will give their enterprise the commissioner’s stamp of approval, thus creating a distinguishing economic asset that is not present in tech-industry currently—namely, trust. There will be trust in the notion that the company will not have obscure privacy settings or that it harnesses personal data for the purpose of unknown exploitations, and finally, trust in the principle that a consumer no longer has to choose between technology and the protection of her online privacy.