Practicing Privacy Online:

Examining Data Protection Regulations Through Google’s Global Expansion

The growth of commerce on the internet has created a paradigm shift where the biggest companies are no longer producers who sell products and services to consumers, but rather data collectors who sell consumers and their information to advertisers. As the largest data collecting corporation—both in terms of sheer size and scope of operations—search engine giant Google has attempted to introduce its increasingly diverse products to every major global market, with mixed success depending on the regulatory framework of the market.

This Note looks at how Google has fared in three of the world’s biggest internet markets—the United States, the European Union, and China—and what its experiences have revealed about each market’s views on protecting the personal data of its citizens online. In light of those experiences, this Note goes a step further in exploring what each data protection regime can do—highlighting the importance of informed user consent—to better achieve, or maintain, a balance between economic and privacy interests in an era of rapidly changing threats to privacy.
INTRODUCTION

Technology companies like Google are primarily based on gathering information, distributing it, and monetizing that process. As such, Google is among the vanguard of a growing industry that allows users to share personal information on an increasingly global scale. However, not everyone wants to share their information, and most people likely do not want to share all of it. In the wake of the industry’s growth has come growing concern over what information is being transferred, to whom, in what ways, and to what degree individual users are aware of that transmission. Accompanying this concern is a vibrant global debate over privacy, with different countries approaching the issue with varied systems, safeguards, and understandings of privacy and the harm caused by violations.

With an increasing amount of our lives spent online—be it professionally, socially, or for other commercial purposes—it is hard to overstate the importance of protecting personal data. Yet the importance of personal data and the approaches to protecting it differ vastly among the governments that regulate the world’s three biggest internet markets. The United States, containing the world’s third biggest—and arguably richest and most innovative—market, avoids sweeping legislation in favor of minimal Federal Trade Commission (FTC) enforcement and a reliance on self-regulation, a sometimes criticized decision in light of the vast information gap between corporations like Google and their customers. The European Union takes a different approach, relying instead on a cohesive framework derived from a single data protection directive. This directive—passed almost two decades ago—has created a regulatory framework that has drawn criticism for being outdated and slow to respond to changing norms. Lastly, the world’s biggest internet market, China, is regulated by a government that has recently begun to pass official legislation protecting the personal data of its citizens, but whose actions indicate a complete lack of regard for anyone’s personal data. While China is impossible to ignore, it is still a long way from being able to join the global discussion on data protection.

These three governments rely on different social, political, and historical norms—often irreconcilable—to craft their distinct privacy policies. However, one empirical idea that this Note will rely on is that of informed consent: the idea that a proper balance of power between corporations and consumers can only be achieved when internet users are empowered with the knowledge of the conse-
quences of their actions. While informed consent need not be coupled with a meaningful choice—for example, an internet user is not given the opportunity to negotiate the terms of a standard privacy policy or consent form so often proffered by internet corporations—taking information from users without their knowledge is destructive to any framework that seeks to protect the user. As such, this Note will address whether the data protection schemes discussed below do in fact conform to the need for informed consent to protect users’ personal data. It is an important point because arguments favoring self-regulation or market forces as an appropriate protection are especially weak if informed consent does not exist in the marketplace.

This Note will examine the data protection schemes of the United States, the European Union, and China to examine how their governments have responded to the new privacy issues that companies like Google have presented. Using Google’s products—which collect and distribute personal information—as a lens, this Note will analyze how these countries’ data protection schemes differ and which country’s scheme seems best suited for the future. First, I will explain why I choose Google, as well as how their products work and potentially pose threats to personal data protection in some countries. Next, I will examine each of the three individual data protection schemes, how they have been developed, and how they have either allowed or challenged Google’s operations in their countries. This Note will also address the different cultural and historical factors in each country that have influenced the development of their privacy policy. Finally, I will make some predictions about how each government might alter its data protection scheme to better balance citizen protection with promoting economic development on the internet in this era of rapid change.

I. GOOGLE: A PIONEER OR BULLY?

So, why Google? Simply put, the company is an ideal repre-

1. The argument by corporations that consumers consent to giving up their personal information is only valid if those consumers actually knew what they were giving up and had a meaningful opportunity to make a choice about it.

2. This Note will show that not all such frameworks are intended to even protect privacy at all.

3. To be clear, this personal information is legally distributed; Google makes sure that it has the user’s consent whenever it is necessary. What is unclear is how aware the user is that she has given consent and what realistic choice a user may have in the future not to consent.
sentative of data-collecting corporations for not only its place as a market and industry leader due to its tremendous success and size, but also its notoriety with privacy issues\(^4\) and its corporate philosophy. For the past several years, Google has maintained an aggressive mission statement to “organize the world’s information and make it universally accessible and useful.”\(^5\) Statements by top executives at the company, such as then-CEO Eric Schmidt,\(^6\) have made it clear that this means all information, including personal data. In a 2009 interview, Mr. Schmidt said, “If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.”\(^7\) Mr. Schmidt’s view that a desire for basic privacy from the world is inherently suspicious\(^8\) has been mirrored by Google’s actions as it has expanded around the globe. More than just Google, the entire world has begun to document and expose every aspect of people’s lives. For example, technology and privacy pundit Evgeny Morozov has discussed this phenomenon in his book, To Save Everything, Click Here: The Folly of Technological Solutionism, which includes discussions of just how much we document and share information, the strangest of which include BinCams, which catalog how well citizens recycle their trash and publicly compares scores across a community.\(^9\) However, while Google aggressively, universally, and seemingly single-mindedly, pursues its mandate, its successes and failures at various points in each of the three countries discussed in this Note are particularly instructive on the state of data

---

4. There is no data on how scrutinized a company is for its privacy practices but it is without question that no company is more scrutinized, domestically or abroad, for its privacy policies than Google.

5. About Google: Company, GOOGLE.COM, http://www.google.com/about/company/ (last visited Mar. 1, 2013). The company’s unofficial motto has jokingly been said to be “Don’t be evil.” While this does not exist on the company’s profile, one of the core beliefs of the company is listed as “You can make money without doing evil.” About Google: Company: What We Believe, GOOGLE.COM, http://www.google.com/about/company/philosophy/ (last visited Mar. 1, 2013).


8. Of course, Google fiercely protects its own corporate secrets—notably the search algorithm that has propelled the company to essentially dominate the internet—leading one to wonder just what Mr. Schmidt meant.

protection across the globe.

What is interesting about Google’s aggressiveness—which again shows why it is a good example here—is that the company’s drive seems to have an ideological component that its peers might lack. In addition to statements like Mr. Schmidt’s and the mission statement, Google’s actions have shown that, while it does indeed turn a tidy profit year in and year out, it often is motivated by more than purely financial factors. For example, in January 2013, Google’s maps product—Google Maps—included for the first time a detailed layout of North Korea, one of the world’s most secretive states. It was the culmination of a two-year project that has no discernible marketable value to Google, but rather represents another successful attempt by the company to make previously inaccessible information available. It is precisely this attitude to leave no stone unturned with regards to information—be it geographic or personal—that makes Google such an interesting lens through which to analyze the data protection schemes of three huge markets that regulate data protection in very different ways.

A. Google Products: Data Collection and Content Creation

Google has a wide range of products that it offers to individuals, the vast majority of which are completely free of charge to the user. The company predominantly makes its money through corporate advertising, which gives companies the opportunity to link their company to certain key words—called AdWords—that are given priority when an individual uses one of Google’s products such as its search function, or Google Maps or Gmail. In other words, Google


11. Although public relations value is always a possibility.


13. Gmail is Google’s free web-based email product. Another Google project that shows this drive is Google Books, in which Google has worked with university libraries to digitize their holdings and make free literary content more easily available to all. There seems to be no commercial value in this project other than perhaps enhancing Google’s overall reputation.

tracks certain information about its individual users in order to tailor advertisements and then charges the advertising companies a rate per advertisement posted. This attracts both parties as the users have access to very powerful online tools for free and advertising directed at their specific interests, and advertisers have a greater ability to target their audiences.

With that basic structure in mind, a few Google products are specifically relevant for the purposes of this Note, namely Google Maps, Google Analytics, and Google Apps, the latter of which uses cloud computing. I will give an overview of each product and how it works, as well as an introduction to the potential threats that each can pose to protecting individual internet users' personal information.

1. Google Maps and Street View

The commonly used Google Maps includes maps, satellite imagery, navigation by car, foot, bike, and mass transit, along with other functions. One primary part of the navigation component of the application is Google recognizing and downloading information about the user's location—whether by GPS on a mobile device or specific location of an IP address for a permanent workstation. Google Maps is free to the user and is considered the standard in online navigation, especially trumping competitors like Apple in the mobile market.15

Furthermore, since 2007, the Google Maps application has included a “Street View” function that allows users to view the buildings and other scenery around specific addresses or locations. In order to capture such images, Google employs special cars that have cameras mounted on top of them.16 These cars simply drive around towns—up and down every street—taking pictures constantly. These pictures are then compiled into 360 degree composites that allow users of Google Maps to get a better sense of the specific area.17

There are two possible privacy concerns with Google Maps and Street View: (1) that the cameras used to compile the Street View images violate citizens’ privacy by photographing people, their


homes and their families, and (2) that one primary component of Google Maps is its ability to geographically locate a user via signals such as IP location, Wi-Fi networks, or GPS without her consent. Both have been heavily challenged in Europe and the Street View program has created very public and embarrassing privacy invasions in both the United States and Europe.

2. Google Analytics

Less well known by the general public but perhaps even more relevant to the privacy discussion is the application known as Google Analytics. A free service, Google Analytics allows a website owner to compile information about visitors to his website and has been credited with revolutionizing the industry of web analytics, which represents the future of online—and perhaps all—advertising. The information collected includes how many visitors a website has, how long the average visitor spends on the site, how many pages the average visitor looks at, how many visitors are new, where the visitor comes to the site from (i.e. search engine, other site, advertisement, etc.), and where the visitor is physically located. As businesses have become more reliant on the internet to both market and sell their products, web analytics has become essential to success online; and Google Analytics is by far the most popular web analytics tool on the market today. The reason for such popularity is partially from the

---

18. See, e.g., David Murphy, Google Abandons Street View in Germany, PCMAG, (Apr. 10, 2011, 2:05 PM), http://www.pcmag.com/article2/0,2817,2383363,00.asp (After extensive litigation, a German court finally ruled that such pictures were not, in fact, a violation of privacy).

19. To clarify, legally, there is always consent given. For example, a user turning on her phone and activating the GPS function is giving consent to track her location. Furthermore, a user give consent when she agrees to the relevant privacy policy. To reiterate, Google is not breaking the law at all in this process. The point here is that users often are unaware that they are giving their consent, which is what worries privacy activists and some regulators.


21. JUSTIN CUTRONI, GOOGLE ANALYTICS ix (2010) ("Web Analytics" is "[t]he analysis of qualitative and quantitative data from your website and the competition, to drive a continual improvement of the online experience that your customers, and potential customers have, which translates into your desired outcomes (online and offline)."").

22. Id. at 5.

23. Matt McGee, Google Analytics Is Installed on More Than 10 Million Websites,
extremely user-friendly interface that allows even the most rudimentary of users to acquire and interpret data necessary to monitoring and increasing traffic and sales at a website.\(^{24}\) It is also free, which quickly eliminated almost every competitor on the market when the product was launched.\(^{25}\)

Google Analytics uses a tracking code, which is a piece of programming code that must be inserted in the programming language of each page on a website.\(^{26}\) When a visitor requests that a certain page be opened in their browser—by clicking on a link or typing the web address into the URL bar—the code activates and downloads a file onto the visitor’s computer.\(^{27}\) This file basically collects certain information about the visitor by accessing information in the web browser.\(^{28}\) It collects information such as how many times the visitor has viewed a page, as well as other useful business data if appropriate.\(^{29}\) This information, once collected by the file, is then sent back to Google—and the owner of the relevant Analytics account—and stored in a manner that Google has not specifically indicated.\(^{30}\) The data is then stored in two different ways: as an individual cookie and as compiled with all the other data to show the website owner the aforementioned information.\(^{31}\) So, any website with Google Analytics essentially has a piece of code on every individual webpage that takes information such as who a visitor is and where they are located every time that the individual visits a webpage.\(^{32}\)

While some expertise with web design is required to install such a code on a website, it is far less complicated a process than designing a webpage in the first place. In other words, anyone with the skill and desire to create a website has the ability to easily activate

\[\text{MARKETING LAND, (Apr. 13, 2012, 2:12 PM), http://marketingland.com/google-analytics-is-installed-on-more-than-10-million-websites-9935 (More than 60% of the top 10,000 websites in the United States use Google Analytics).}\]


\[25. \text{While Google does not draw any revenue directly from this product, it certainly promotes the usage of Google’s main revenue source: AdWords. See id.}\]

\[26. \text{CUTRONI, supra note 21, at 13.}\]

\[27. \text{Id. at 14.}\]

\[28. \text{Id.}\]

\[29. \text{Id.}\]

\[30. \text{Id. at 14–15.}\]

\[31. \text{Id.}\]

\[32. \text{Id. at 15.}\]
Google Analytics for his website and thus effectively take some information from any visitor; and throughout the process, Google collects all of it. It is very similar to the owner of a billboard being able to track every person who views that billboard by recording the license plate of every car driving by, what time they drove by, and how many times they have driven by—how much information would the company that collected all of this data have? It is a very powerful business tool, a potentially invasive collection of personal information, and completely legal in the United States. Lastly, unlike a GPS location for Google Maps, about which a user is notified and which can be effectively turned off, Google Analytics does not ever notify the visitor that their information is being collected, nor is there an obvious way to turn off such data collection, although it is possible. While this is a somewhat simplified version of the process, it does illustrate the data protection concerns addressed later in this Note; predominantly the growing information gap between users and providers, which prevents the user from giving informed consent to the taking of their personal information due to ignorance of the process.

Similar to the data acquired by Google Analytics are the files known as “cookies,” which are basically text files that are stored on an individual user’s computer and remember the user’s preferences on that website. They can be used to remember passwords, recent articles read, or interests expressed, and generally allow a website to recognize returning individual users. They can be very useful to website owners and visitors alike. Cookies help a website owner customize their website based on the information in the cookie—such as tailoring advertisements to interests previously expressed by the visitor and saved in the cookie. Cookies can help a website visitor by enhancing their experience as a cookie stores the user’s prefer-

33. Google Maps asks the user if it can access their location before doing so, and any mobile version of the application can be turned off by the user simply by deactivating the GPS on their mobile device. See Enable Location Services, GOOGLE, https://support.google.com/gmm/answer/16461407?hl=en (last visited Nov. 5, 2013).

34. Although, as noted elsewhere, a cookie can be deleted and users can disable the cookies or JavaScript to prevent such action. See CUTRONI, supra note 21, at 31.

35. For a more in-depth description of the process and web analytics as a whole, see CUTRONI, supra note 21.


ences—such as passwords, recently purchased products, and other useful information. \(^{38}\) Cookies can be turned off by the user if desired, but they are so prevalent in the United States that websites often might not work properly if cookies are disabled. \(^{39}\) In general, American views on cookies trend towards accepting the data that they collect as the cost of receiving so much free content online. \(^{40}\) To wit, they are often described as rather harmless: "[c]ookies are not software. They can’t be programmed, can’t carry viruses, and can’t unleash malware to go wilding through your hard drive. Only the Web site that sent you the cookie can read it. As soon as you leave a site, its cookie sits dormant, waiting for your return." \(^{41}\)

3. Google Apps and a Shift to Content Creation

While the company first made its name as an internet search engine, Google’s pursuits have diversified greatly in the past decade. Most notable perhaps is Google’s entrance into the mobile device market with its Android line of smart phones and tablets. However, Google has also made a serious commitment to content creation. \(^{42}\) In other words, in addition to trying to collect, organize, and distribute existing information on the internet, Google is attempting to ensure that future information—be it YouTube videos, books, music, or business related documents—is created within the company’s network and, thus, control. Google has certainly faced significant hurdles in this market, most notably with Google Plus, a social media product intended to compete directly with Facebook. \(^{43}\) Yet Google has not backed away and continues to support both Google Plus and other ventures in content creation. \(^{44}\)

In terms of its products for businesses, this goal manifests itself as the product Google Apps, one of the few products for which

---

38. Id.
41. Id.
44. See id.
Google actually charges the user. Google Apps is a cloud-based collection of Google products designed to help businesses with their communications and data storage. Individual products in the package include Gmail, Google Calendar, Drive, Docs, and Sheets. These products are simply Google’s online version of Microsoft Outlook (with email and calendar), an external hard-drive, Microsoft Word, and Microsoft Excel, respectively. It is essentially a product for businesses that directly competes with Microsoft Office, the major difference being that all information in the Google system is stored remotely using what is called “cloud computing.” This aspect is often a selling point because it is easier for businesses to use Google Apps as it can be accessed from anywhere that has an internet connection; it does not require the business itself to invest in data processing or storage hardware; and it is protected by Google security rather than relying on an in-house system, as Google provides all of that offsite. On the other hand, there are certain concerns, discussed below, that users will lose control of all the information contained in company documents and emails, thus ceding that control to Google. Google currently claims that five million businesses use the product.

4. The Cloud: Data Storage and Load Balancing

Cloud computing represents the next step in the evolution of data storage as a third party endeavor, rather than something that businesses do for themselves. One author compares it to the industrial revolution, when factories went from producing their own power


47. *See infra* Part I.A.4. Microsoft has recently started heavily marketing its “SkyDrive” product, which directly competes against Google Apps by allowing users to save Office documents via cloud storage.

48. *Id.*

49. *Id.*


to hooking up to a newly formed electric power grid. Another way to think about it is storing all of your money—here, information—in a bank rather than in your home or business. Simply put, economies of scale make it more efficient and cost effective for many firms to store the massive amount of data that they generate with third party networks that offer both vast amounts of space and security, rather than on their own mainframes. Four major providers of such storage services are Amazon, Google, Microsoft, and Salesforce. To create such extensive storage networks, these corporations (and others) maintain data centers, individually capable of processing massive amounts of data, all over the world. Google alone has centers in Ireland, Belgium, Hong Kong, Singapore, Taiwan, Chile, Finland, and six in the United States. These centers work together to create a network within which data can be moved around and efficiently stored and protected.

One function of cloud computing that is important to the issues discussed in this paper is automatic scaling and load balancing. In order for Google’s thirteen data centers to maximize efficiency, they automatically distribute the information, also termed data “clusters,” uploaded to the “cloud,” so as to balance the level of storage and performance at each facility. This flexibility is considered a “highly desirable feature,” but it also prevents Google—or the information owner—from knowing where information is, or will be, physically located at any given point in time. While Microsoft claims that it provides for “discovery”—that is, being able to physically locate the data or otherwise guarantee its whereabouts—that capability is very limited at this time. This becomes an issue against the backdrop of European Union data protection policies stating that personal information must physically be stored in certain locations.

53. This analogy is slightly more appropriate as users are storing something important to them with professionals, both for safety and for ease of access around the world.
56. See Voorsluys et al., supra note 52, at 26–27.
57. See id.
58. Brock & Gosinski, supra note 54, at 196.
59. See infra Part III.A.
II. LAND OF THE "FREE": AMERICA'S PATCHWORK PRIVACY QUILT

The United States has no single agency responsible for protecting individuals' personal data online, either from the government or from corporations. Rather, a combination of federal entities, primarily the Federal Trade Commission and the Department of Commerce, has worked together to provide a piecemeal privacy framework, although other departments have also gotten involved to a lesser extent. The patchwork scheme relies partially on legislation, administrative oversight, and, predominantly, self-regulation.

A. Legislation

In terms of legislation, the United States has been averse to any kind of comprehensive legislation regulating data protection. Three recently proposed—and subsequently abandoned—congressional bills that would create a more centralized framework for regulating certain types of personal data collection online show the reluctance of Congress to seriously consider such a scheme. The BEST Practices Act, in part, would have required opportunities for internet users to opt out of their online activity being tracked, along with requiring that data collectors make privacy policy disclosures that were easy to read and comprehend by the general public. The Commercial Privacy Bill of Rights Act of 2011 would have essentially empowered the FTC as the central regulatory agency regarding data protection, compelling the Commission to promulgate rules regulating data collectors and the options that they were re-

quired to provide to internet users.\textsuperscript{65} The Consumer Privacy Protection Act of 2011 would have compelled data collectors to issue and update privacy policies to all users from whom they would potentially collect data.\textsuperscript{66} Despite two out of three polled Americans stating that they do not believe that online advertisers should be able to collect their information,\textsuperscript{67} as of this printing, Congress has yet to respond to that data, or any other pressure from privacy watchdogs, to seriously consider centralized legislation regarding data protection. Rather, the United States has continued to rely on corporate self-regulation that is based on a paradigm of "notice and consent,"\textsuperscript{68} with an apparent lack of notice.

On the other hand, two scholars have recently articulated an argument that, while the patchwork statutory scheme leaves much to be desired on its face, in practice, privacy regulation "on the ground" actually works in protecting consumers. The authors concluded that:

\begin{quote}
[P]ursuing [a uniform privacy scheme] in a way that eclipses broader robust substantive protections, or constrains the regulatory flexibility that permits their evolution, may destroy important tools for overcoming corporate overreaching, consumer manipulation, and the... problems raised by ceding privacy protection exclusively to the realm of individual choice.\textsuperscript{69}
\end{quote}

In other words, the argument is that a single comprehensive privacy framework will not be flexible enough to efficiently cover many situations in which both consumer and corporate interests may be at risk. This argument seemingly looks at the European approach, discussed in Part III, as a cautionary tale of what happens to corporations under a centralized privacy regime. Alternatively, the article proposes that current administrative regulation by government agen-

\textsuperscript{65} See id. at 329–31.
\textsuperscript{66} See id. at 331–32.
\textsuperscript{67} Gallup Poll asking, “[Advertisers tailor advertisements] by collecting data that shows what websites you have visited. Do you think advertisers should or should not be allowed to do this?” To which 67% of respondents answered, “[They] should not.” Computers and the Internet, GALLUP, http://www.gallup.com/poll/1591/Computers-Internet.aspx#2 (last visited Nov. 4, 2013) (the survey itself was performed from December 10 to December 12, 2010).

\textsuperscript{68} Although it should be noted that such a paradigm may be starting to shift. See Stephanie Clifford, \textit{F.T.C.: Has Internet Gone Beyond Privacy Policies?}, N.Y. TIMES MEDIA DECODER (Jan. 11, 2010, 4:03 PM), http://mediadecoder.blogs.nytimes.com/2010/01/11/ftc-has-internet-gone-beyond-privacy-policies.

cies and self-regulation provide a sufficient framework to safeguard the privacy of American internet users without constraining corporate interests. However, it does not address the issues of informed consent and whether the market is even capable of self-regulation when consumers are not fully aware of what they are giving up.

B. Administrative Regulation and Enforcement

In terms of administrative oversight and enforcement, online data protection is generally overseen by the FTC and—to a lesser extent—the Department of Commerce and others,\(^70\) which are often aided by the Department of Justice.\(^71\) None of these departments, however, focus solely on data protection and, perhaps as a result, there have been instances where the FTC’s ability to truly regulate and enforce data protection has been questioned.\(^72\) The Commission has recently made strides to provide guidelines and recommendations for businesses and policymakers regarding data protection.\(^73\) However, that report has been criticized by some who note that the Commission still “mistakenly endorses self-regulation . . . and fails to explain why it has not used its current Section 5 authority to better safeguard the interests of consumers.”\(^74\) In fact, when it comes to enforcement, the FTC was itself sued by the privacy watchdog, the Electronic Privacy Information Center (EPIC),\(^75\) for not enforcing a settlement made with Google in 2011.\(^76\) While the FTC has recently

---

70. Other administrative agencies, such as the Federal Communications Commission (FCC), have also investigated Google over privacy concerns. The FCC specifically has done so over Google Maps Street View. See FCC Investigation of Google Street View, EPIC.ORG, http://epic.org/privacy/google/fcc__investigation_of_google_st.html (last visited Mar. 3, 2013).

71. See Swire, supra note 60.


75. EPIC is one of the FTC’s biggest critics and is responsible for the quote cited in the note 74, directly above.

76. Jessica Guynn, Watchdog Sues FTC over New Google Privacy Policy, L.A. TIMES,
been actively investigating Google for the past two and a half years, that action has involved antitrust issues, which the FTC also enforces, and not privacy concerns.\footnote{77}

Also notably unsatisfied by the FTC’s enforcement are the attorneys general and governors of many states in the United States. Notably the Connecticut Attorney General, George Jepsen, has taken an active role in both enforcing data protection violations,\footnote{78} and pushing for legislation that would better protect consumer privacy for Connecticut citizens.\footnote{79} Connecticut has been joined by thirty-six other states and territories in voicing concern over Google’s recent privacy policy—published in 2012—and has contacted Google directly about its concerns.\footnote{80} Also noteworthy for taking independent steps to protect its citizens’ personal data has been California, where the Attorney General recently established a Privacy Enforcement and Protection Unit.\footnote{81} The unit, like Connecticut’s established in 2011,\footnote{82} has a broad mandate and reflects one of State Attorney General Kamala Harris’s “top priorities.”\footnote{83} The involvement of state attorneys general, in response to non-enforcement by the FTC, could potentially create discrepancies in privacy policy by state that could greatly hinder business development online. Even those in support of the current enforcement framework admit that “the ambiguous legal standards grounding the Commission’s most powerful exercise of its regulatory power render enforcement unpredictable and incom-


\footnote{82}{See Press Release, Office of the Attorney Gen. of Conn., \textit{supra} note 79.}

\footnote{83}{See Press Release, Office of the Attorney Gen. of Cal., \textit{supra} note 81.}
C. Self-Regulation

Because of the dearth of legislation in the area and an apparent unwillingness to find the limits of its enforcement power, the FTC has "promoted industry self-regulation in the field of online behavioral tracking." Indeed, there are arguments that the market itself, and a need to maintain consumer trust, would compel corporations to promulgate and follow sufficient safeguards to internet users' personal data. Corporations like Google have offered "Do Not Track" options on their web browser—Google Chrome—that allow internet users to prevent the program from tracking their online activities. However, a universal lack of transparency by corporations has rendered the market uninformed and thus an ineffective method of data protection. Users simply do not read the information given to them—usually through long and convoluted privacy policies—and thus are often unable to make informed choices about whom they can trust. In fact, to date, the market has provided such little incentive for self-regulation that the FTC has recently asserted that "efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection."

A 2011 interview with privacy advocate Professor Eben Moglen at Columbia Law School highlights the failure of self-regulation: individuals within the market are unable to protect themselves due to a lack of understanding. Moglen and other privacy advocates seem to fear that once internet users begin to give away the rights to their privacy, those rights become nearly impossible to get back. In other words, they believe that corporations are taking advantage of

84. Bamberger & Mulligan, supra note 69, at 310.
85. Tene & Polonetsky, supra note 64, at 314 ("Online behavioral tracking" is essentially what online advertisers do with data collected from online users).
88. Tene & Polonetsky, supra note 64, at 314.
89. Id. at 315.
91. See id.
“self-regulation” and commercially benefitting because such a form of regulation itself is impossible to achieve due to a lack of informed consent.

 Exactly why the United States has avoided any centralized authority on privacy and, more specifically, data protection, is not entirely clear, although one author credits a general “American disdain for big government” as creating an environment that relies predominantly on self-regulation.92 This argument is highlighted by recent controversy surrounding the government’s acquisition of personal data from mobile carriers, predominantly Verizon.93 While there has been massive outcry against the U.S. government—highlighted by concerns about it becoming “big brother”—in response, there have not been any complaints that Verizon has gathered this information in the first place, or that it has given it away without more of a fight.94 Both the press and the public seem completely comfortable with Verizon—a corporation explicitly geared towards profiting off of the public—having all of their information, but incensed at the idea that public servants might have access to portions of that same information that was already so willingly given away. This perspective is in stark contrast to other countries discussed below, whose populations seem to trust their governments more than the for-profit corporations in their respective countries.

 Regardless of the reasons for the unique U.S. stance, American legal scholars are in the minority in advocating for the creation of a more centralized authority on data protection in the digital age.95 The Department of Commerce’s Internet Policy Task Force has chimed in too, recommending a new framework that “articulate[s] certain core privacy principles—in order to assure baseline consumer protections.”96 Other scholars have supported this finding, adding the Executive Office of the President as a possible home for such an


95. See generally Bamberger & Mulligan, supra note 69, at 256–60.

authority and citing the need for such centralization both domestically and so as to articulate a single stance in the international community.97

The lax regulatory framework in the United States has allowed corporations in America to gather more information about domestic consumers than anywhere else in the world. While this environment has certainly allowed companies such as Google, Amazon, and similar internet-based companies to thrive domestically, it can certainly create hurdles when such corporations venture abroad and encounter much more rigorous guidelines apart from privacy issues. Additionally, setting aside a company’s ability to satisfy foreign guidelines, the lax regulation in the United States certainly makes European regulators wary of American corporations as a whole.98 It also poses concerns as to how such a decentralized framework will be able to respond to what the FTC has appropriately coined an “Era of Rapid Change” for privacy threats.

III. THE SAFETY NET: THE EUROPEAN UNION’S CENTRALIZED DATA PROTECTION SCHEME

A. The Framework of the 1995 Directive

In stark contrast to the United States, the European Union and its members have adopted a single data protection directive that creates a comprehensive regulatory scheme for protecting the privacy of its consumers from corporations.99 One author has suggested that the more stringent privacy regulations concerning personal information are remnants of the region’s “grisly past” regarding persecution of Jewish citizens based on “extensive government records of citizens’ personal information.”100 However, this view does not seem to be widely—or at least publicly—shared. Regardless of the reason, European citizens (and European leadership) are very concerned with protecting personal information from corporations today, especially as technology develops and smartphones become more prevalent. At

97. Swire, supra note 60, at 49.
98. Google itself is a prime example of this distrust as it has drawn a disproportionate level of scrutiny from European regulators.
the Third Annual European Data Protection and Privacy Conference in Brussels in December 2012, the Vice-President of the European Commission stated in a speech that:

[W]e have to think about whether our data protection rules still work. Many citizens think that they don’t. 92% of Europeans are concerned about mobile apps collecting their data without their consent. 89% of people say they want to know when the data on their smartphone is being shared with a third party. They want the option to give or refuse permission. This raises an important question. A question which goes to the heart of this new economy. Can it continue to grow without the trust of citizens? The citizens on whose data it depends. ¹⁰¹

While no exactly analogous data is readily available, American Gallup polls indicate these figures are even higher than similar ones in the United States. ¹⁰² The attitude that Europeans have towards data protection is enshrined in the Charter of Fundamental Rights of the European Union—a fundamental document to the political organization—which states that every person has both the right to respect for her private life, home and communications, all personal data, and the right to rectify any instances of misappropriation of such data. ¹⁰³

From the very beginning, the European Union has been aware of the risks to personal data posed by computers and the internet. While the United States has added piecemeal legislation and regulation, the European Union—from the very outset of the internet’s rise in popularity—has relied on a top-down comprehensive statutory framework. The European Union’s first data protection directive, passed in 1995, provided a uniform framework for protecting the privacy of personal data in the European Union’s then-fifteen member states. The 1995 Directive, ¹⁰⁴ while allowing further regulation by

¹⁰². GALLUP, supra note 67.
¹⁰⁴. The European Parliament is empowered to issue directives by the Treaty of Lisbon, which states that “[1]o the extent necessary to facilitate mutual recognition of judgments and judicial decisions . . . the European Parliament . . . may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules.” Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European
individual nations so long as it did not restrict the flow of information within the European Union, has an exclusive list of six possible reasons for processing personal data:

(1) If the subject provides unambiguous consent, (2) if it is pursuant to a contract entered into by the subject, (3) if there is a legal obligation to do so by the processor, (4) if it is necessary to "protect the vital interests" of the subject, (5) if it is pursuant to the public interest or "in the exercise of official authority," and (6) legitimate interests pursued by one to whom the data has been disclosed so long as it does not override any of the subjects rights and freedoms.  

More succinctly put, the original framework was intended to allow processing of personal data in a very limited number of situations, generally involving either a legitimate governmental purpose, or consent or need by the subject of the personal data. Furthermore, except in limited enumerated circumstances, there is a ban on processing personal data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and... health or sex life [data]." All of these restrictions are stricter than any in the piecemeal U.S. legislation and show that, from early in the internet era, the European Union had a focus on promoting economic development and sharing information across national boundaries. Moreover, the restrictions show that the European Union placed more of a premium on universally protecting what it considered to be a fundamental right to exclusive ownership of personal information absent legal necessity or explicit consent otherwise by the subject. The Directive also forbids the storage of personal data

Community art. 69A(2), 2007 O.J. (C 306) 1. Simply put, directives "lay down certain end results that must be achieved in every Member State. National authorities have to adapt their laws to meet these goals, but are free to decide how to do so." In other words, they ensure a certain level of uniformity while allowing discretion to individual nations. Application of EU law: What are EU directives?, EUROPA, http://ec.europa.eu/eu_law/introduction/what_directive_en.htm (last visited March 3, 2013).

105. 1995 Directive, supra note 99, Section II.

106. Examples include (1) explicit consent, (2) protecting the subject’s vital interests, and (3) legal proceedings or other likewise legitimate purposes. See 1995 Directive, supra note 99, Section III.

107. Id.

108. Subsequent follow up communications from the Commission of the European Communities indicate that the parties involved believed that the Data Protection Directive "set a milestone in the history of the protection of personal data as a fundamental right." Comm’n of the Eur. Cmty., Communication from the Commission to the European
outside of the European Union or any country deemed to have an equivalent data protection scheme, reflecting the lack of popularity of the internet at the time of passage.\textsuperscript{109}

Particularly of note in the E.U. legislation is the language that allows data processing so long as it is done pursuant to a "legitimate government interest."\textsuperscript{110} These provisions indicate that E.U. legislation is primarily aimed at preventing corporations from collecting personal data, with large swaths of exceptions carved out for governmental action. While it is unclear just how broadly E.U. regulators and courts would interpret language "in the exercise of official authority,"\textsuperscript{111} it is clear that the European Union is more concerned with corporate malfeasance than governmental misappropriation of personal data. This priority is in contrast to those of their American counterparts.

The broader E.U. framework has created a floor for protection and allowed for national legislation while establishing individual data protection authorities in each member state. The Commission of the European Communities has engaged in seemingly constant dialogue with such authorities to ensure consistent legislation across the European Union while promoting closer regulation of industries using personal data—such as private insurance—as well as "privacy enhancing technologies."\textsuperscript{112} Notably, while the European Union has attempted to promote self-regulation through codes of conduct by industry federations, apart from simply raising awareness of privacy issues among businesses and individuals, the Commission has noted that attempts to promote more self-regulation have failed.\textsuperscript{113}

While attempts at promoting better self-regulation have fallen short, one notable success of the 1995 Directive has been the creation of the "Working Party on the Protection of Individuals with regard to the Processing of Personal Data." Established by Article 29 of the 1995 Directive, and known simply as the Article 29 Working Party (the "Working Party"), the group is comprised of at least one member of each member state's data protection authority and acts inde-

\textsuperscript{109} 1995 Directive, \textit{supra} note 99, art. 2 (d).
\textsuperscript{110} \textit{Id.} art. 7 ¶ (e).
\textsuperscript{111} \textit{Id.}
\textsuperscript{112} See \textit{supra} note 108.
\textsuperscript{113} \textit{Id.}
pendently as an advisor. The goal of the Working Party is to ensure that the various member states of the European Union remain consistent with each other in legislating pursuant to the 1995 Directive. This group is an example of the top-down uniformity that the European Union seeks to promulgate and—as discussed below—can be critical in helping to explain and remedy various inconsistencies in privacy regulation throughout the European Union.

Notably, however, the Working Party is generally comprised of politicians and lawyers with backgrounds in a broad spectrum of fields, including law enforcement, civil engineering, human rights, political science, social policy, foreign affairs, economics, and mathematics. While there are some members who have dedicated their education and professional careers to information technology and data protection—particularly the members from Austria, Germany, France, and Latvia—the leadership of the Working Party, as well as its general membership, do not reflect any such expertise. In other words, the composition of the Working Party indicates a pronounced lack of experience with current data protection, especially the new and ever-changing privacy issues that arise concerning the information superhighway that is today's internet.

Overall, while both the language of the 1995 Directive and subsequent policy make it clear that the European Union acknowledges that acquisition of personal information is necessary to facilitate economic growth, it also puts a premium—one that American legislation lacks—on protecting information and informing the individual internet user. Furthermore, it provides a single regulatory framework that the twenty-seven member states of the European Union adhere to while crafting their own individual data protection schemes. In short, the twenty-seven countries that make up the European Union have a more cohesive strategy for protecting personal

114. 1995 Directive, supra note 99, Ch. VI, art. 29.
115. See id.
117. See id.
data than the different departments within the United States federal government have created. However, the mechanism does not always operate as smoothly—or promote as much consistency—as the framers of the directive probably intended.

B. Legislation Under the E.U. Regime: The "Cookie Directive"

Perhaps the best way to explain how E.U. policies are created is a quick case study of the much maligned "Cookie Directive" that has drawn rage and ridicule from American privacy pundits and corporations alike. As previously discussed, cookies are text files that carry information about the visitor's prior activity on a specific website.119 A 2002 Directive, intended to supplement the original 1995 Data Protection Directive, has acknowledged that cookies "can be a legitimate and useful tool."120 However, the law proscribed that cookies only be "allowed on the condition that users are provided with clear and precise information... about the purposes of cookies... to ensure that users are made aware of information being placed on the terminal equipment they are using."121 The 2002 Directive required that all users should have the opportunity to refuse having a cookie "or similar device" used to store their information and that such a choice should be made "as user friendly as possible."122 This stance on the value of cookies versus the threat that they pose as a danger to the privacy of personal data is in stark contrast to the American perception of cookies as benign.123

More recently, a 2009 Directive on cookies tightened the requirements of the 2002 Directive mentioned above by requiring each website to get a user's direct consent every time it wants to store cookies on their computer.124 The 2009 Directive has drawn anger and ridicule from many U.S. and British technology bloggers, who see the law as an affront to both the information sharing and econom-

119. See supra I.A.2.
121. Id.
122. Id.
123. Penenberg, supra note 40.
ic goals of the internet. Critics mocked the European regulators as "octogenarian lawmakers who couldn't use a mouse" and generally bemoaned the constraints that the regulation would put both on commercial operations and general ease of browsing. The age of the regulators aside, the Directive did pose a serious problem when E.U. members' interpretations of the 2009 Directive were scattered, creating discrepancies between different countries' policies that any business hoping to do business in the European Union would have to sort out. Two years into the process, the Working Party issued an advisory opinion covering enforcement and "[s]ome clarifications regarding cookies and consent" that sought to promote uniformity throughout the process. The opinion included types of cookies that were exempt from the 2009 Directive as well as methods of gaining consent that were less invasive to the browsing experience than the commonly used "pop-up" window that is such a pestilence that most browsers automatically block it. Still, as of publication of this Note, the Directive's one year grace period has expired and the various countries' cookie laws should be in effect, although it is unclear if any prosecutions for non-compliance have actually occurred.

The process of legislation and enforcement pursuant to the 2009 Directive has been heavily criticized and cannot be how its drafters hoped it would be received. Furthermore, it is likely not a one-time anomaly. However, there are several takeaways that would indicate that the framework itself could work, despite the execution and policy problems with this particular legislation. For starters, the various data protection agencies stayed within the framework while responding to local concerns. Furthermore, the Working Party's

125. See Silktide, The Stupid EU Cookie Law in 2½ Minutes, YouTube, http://www.youtube.com/watch?v=arWJA0jVPAc (last updated May 31, 2011); see also, James Cooper, The History of the EU Cookie Law [Infographic], (Feb. 11, 2013), http://churchm.ag/eu-cookie-law-history/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ChurchCrunch+%28ChurchCrunch%29 (derogatory infographic captures technology pundits' scorn for European ideas of privacy protection).

126. See Cooper, supra note 125.


129. Id.

130. For the British data protection authorities response, see, e.g., Cookies Regulations
clarifications—while not sufficient to resolve all of the issues with the legislation—did respond to concerns, clarify a centralized opinion, and offer suggestions for enforcement.131 Bluntly put, the initial legislation was so poorly received—and, if its critics are to be believed, poorly conceived—that it seems to have never had a chance of success in the first place.132 This kind of failure seems to reflect more on the specific legislators who passed such a directive, rather than on the system overall.

C. Regulation and Enforcement under the 1995 Directive: Germany’s Data Protection

Under the 1995 Directive, member states were given a regulatory floor but were otherwise left to create their own regulatory and enforcement agencies that would carry out the policy of the directive at the national level. This manifested itself in the creation of differently named but similarly contrived agencies throughout the continent.133 Because Germany contains the single biggest market in the European Union, as well as influence over other European data protection agencies and general E.U. policy decisions,134 the German data protection authority is a good example here,135 as companies like Google have made exceptions for Germany that they have not made elsewhere.136 It has also had a fair number of conflicts with Google that highlight important characteristics of European regulation as opposed to regulation elsewhere.

The governing statute for data protection in Germany is the Federal Data Protection Act, passed in 2003 and last amended in 2009.137 Beyond the requirements of the 1995 Directive, the German

---


132. See Silktide, supra note 125.

133. For example, France’s agency is the Commission nationale de l’informatique (CNIL), England’s agency is the Information Commissioner’s Office (ICO), Italy’s is the Garante per la protezione dei dati personali, etc.


136. See infra III.C.1.

137. Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der
legislation requires every company that processes data to employ a data protection official to monitor the company’s data processing to ensure proper privacy considerations are met. It also includes provisions for the general administration and election of the German DPA’s offices and positions. What is interesting in Germany is that there is a division of power between the federal government and the different states who each have their own legislation and enforcement agencies. This throws into sharp relief a major potential—yet seemingly not-criticized—flaw in the 1995 Directive’s aim of consistency. While the 1995 Directive sets a floor for regulation above which all member states must set their own policies, there is no ceiling on data protection, which allows countries to pile on regulations beyond E.U. norms and, perhaps, common sense. Under the German system, the federal data protection authority oversees the German federal government and private telecommunications and postal services companies, while state data protection authorities oversee municipal governments and other businesses.

1. German Enforcement: Conflicts With Google

As a result of Google’s dominance in certain markets, both federal and state data protection authorities have some oversight of the company as it is used by both federal and state agencies. Many of the conflicts that Google has had with German regulators have directly mirrored, or at least echoed, similar issues in other countries. However, this first conflict—regarding Google Maps—is unique in some respects to Germany, most likely because Google was willing to make concessions to such a large market that it would not other-


138. Id. § 4g.
139. Id. §§ 22–26.
140. See Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, LDI.NRW, https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Aufsichtsbehoerden/Aufsichtsbehoerden.php (last visited Mar. 4, 2013) (one state’s website shows the links to the other fifteen state data protection agencies).
wise make. That plan backfired.

After the success of its Street View application in the United States, Google attempted to bring the product to Germany in 2010. While Google claims that there was a huge demand for the service in Germany, it faced a litany of legal complaints from German citizens alleging invasions of privacy by the Google photograph cars. Google, ostensibly out of a desire to ingratiate itself with the desirable German market, made a then-uncommon decision to tailor its privacy policy and allow individuals to opt out of having their homes displayed on the Street View function—primarily by simply blurring those parts of the composite pictures—even though it was seemingly not obligated to do so. It was a catastrophe. With over 244,000 people opting out immediately through a somewhat convoluted system, Google abandoned the expansion in early 2011, leaving only about 20 cities documented in Germany. There was even a grassroots pushback of sorts against Street View that turned out to be quite comical: Norwegian citizens—presumably ones with time on their hands—took to chasing around the easily identifiable Google Street View camera cars while dressed up in silly outfits such as full SCUBA suits, or with pitchforks. German citizens perpetrated similar hoaxes mocking Google’s efforts. The intent was no doubt

143. To be fair, reports from around the time indicate that Google had about 95% of the search market in the country. See Heather Horn, Germany’s War with Facebook and Google Over Privacy, ATLANTIC (Dec. 2, 2011, 11:25 AM), http://www.theatlantic.com/international/archive/2011/12/germanys-war-with-facebook-and-google-over-privacy/248914/.


145. Id.; see also David Murphy, Google Abandons Street View in Germany, PC MAGAZINE (Apr. 10, 2011, 2:05 PM), http://www.pcmag.com/article2/0,2817,2383363,00.asp.

146. In order to confirm that the person requesting the opt-out was in fact a resident at the address in question, Google would mail out a letter to the address in question. The resident would then go to a website specified on the letter in order to confirm residency and complete the process. However, for multi-family homes and multi-purpose buildings—such as ones containing businesses that wanted to be listed but residents who did not—the opt-out process caused a dilemma that eventually helped force Google to abandon its Street View agenda in Germany. See Kremp, supra note 144.

147. Murphy, supra note 145.

to be absurd, rather than activist, but worth mentioning as a cultural pushback of sorts against Google’s attempts. Rather than merely a failure to please regulators, the Google Street View debacle is a perfect example of a total failure—on a cultural and legal level—to bring a previously successful product to a new market.

While the specifics of the Google Street View incident were unique to Germany, Greece and certain non-E.U. countries\(^1\) have also challenged the product. Google has also faced several other hurdles in Germany that it has seen elsewhere in Europe. Notably, in 2009, the data protection authority of the state of Hamburg, along with federal authorities, announced concerns that Google Analytics was in violation of the country’s data protection policies.\(^2\) After two years of working with German authorities, both Google and German companies made concessions that satisfied all parties involved, and the issue was resolved.\(^3\) In short, the product was legal as long as German website operators (1) informed their users that Google Analytics was used on the website, (2) took advantage of Google-provided options to make captured IP addresses anonymous, and (3) offered users an option to disable the Google Analytics tracking code.\(^4\) Note that while the process drew confusion and, perhaps, consternation from Google, as well as criticism for being short-sighted from tech bloggers, a resolution was reached through cooperation—albeit seemingly contentious at times\(^5\)—without any penalties being imposed on any parties.

Lastly, while Germany has never officially declared Google

---


152. Bas van den Beld, Google Analytics Can Be Used in Germany Without Complaint, STATE OF DIGITAL (Sept. 26, 2011), http://www.stateofdigital.com/google-analytics-can-be-used-in-germany-without-complaint/.

153. Id.

154. Google was “not aware that discussions with the German authorities were over.” Google Analytics May Be Banned in Germany, DIGITAL DEFENCE, http://digital-defence.com/news/google-analytics-may-be-banned-germany (last visited March 4, 2013).
Apps illegal, it has expressed serious concerns with the product's cloud-based storage system. There were two primary pieces of legislation that worried the German government: (1) compliance with the 1995 Directive provision that all personal data collected need be stored in the country of origin, and (2) the United States PATRIOT Act. Because Google uses a "load balancing" system of data storage, it has no real way to determine where its stored data is physically located at any given moment. This means that Google cannot guarantee that the 1995 Directive provision, which requires that all data physically stay within the European Union, is fulfilled. Furthermore, the United States PATRIOT Act would allow the U.S. government to compel disclosure of personal information stored by companies with sufficient ties to the United States—such as internet giants Google, Amazon, and Facebook—regardless of where such information is stored. This poses obvious privacy concerns for Germany and other E.U. members, as Google and Microsoft have both admitted that they would comply—and in some instances already have complied—with U.S. requests for personal data pursuant to the PATRIOT Act. German concerns over such possible privacy violations have understandably not been criticized like other German challenges have been.

2. Enforcement Elsewhere in the European Union

Germany is not the only country in the European Union to have had issues with Google concerning data protection. Most notably, Greece has had privacy concerns regarding Google Street View.


156. See supra Part I.A.4.

157. Id.

158. Id.


similar to those held in Germany, albeit with less accommodation from Google.\textsuperscript{161} This issue, first reported in 2009, is still unresolved in Greece as of publication. Google has neither announced abandonment of the project, nor has Greece been mapped, as is evident from a quick search of Google Maps.\textsuperscript{162}

Also notable is the trial of Google employees in Italy in which three executives—two legal executives and a former chief financial officer—were convicted of violation of privacy.\textsuperscript{163} The case revolved around a video posted to Google’s subsidiary YouTube, which showed an autistic child being harassed and bullied by others.\textsuperscript{164} The ruling was based on the Italian privacy law that “prohibits the use of someone’s personal data with the intent of harming him or making a profit.”\textsuperscript{165} Had the ruling stood, it would have set a precedent for holding a web host accountable for all content uploaded by users, effectively forcing Google to monitor every video uploaded to YouTube.\textsuperscript{166} Nearly two years later, an Italian appellate court overturned the ruling, but the Italian Attorney General stated that she was unsure if she would appeal the decision further.\textsuperscript{167} Had the decision been upheld, seemingly any distribution of a person’s likeness without that person’s consent would have been considered in violation of Italy’s stringent privacy laws. The ramifications of having to comply with such a policy would have made YouTube in Italy—and anywhere else that followed suit—commercially untenable, leaving one to ponder how Google would have responded if the appellate court had upheld the decision.

It is worth mentioning that for all of the privacy battles that Google has faced, twelve different countries (including the United States) have investigated the company for privacy abuses committed


\textsuperscript{164} Id.

\textsuperscript{165} Id.

\textsuperscript{166} This would be an impossible task as Google claims that 20 hours of video is uploaded to YouTube every minute. See id.

by its Google Street View mapping cars.\textsuperscript{168} Simply put, the cars that
Google had sent driving along the streets of so many cities around the
world had been grabbing personal data from any individual Wi-Fi
network that they encountered.\textsuperscript{169} In addition to gathering physical
information in the form of pictures, Google was effectively hacking
into every network that it could to mine for data.\textsuperscript{170} Google claims
that the flagrant violations were the result of a piece of programming
code mistakenly written into the software put into the Street View
cars and it has expressed remorse in cooperating with authorities to
delete the data collected and remedy the situation.\textsuperscript{171} Regardless, the
event shows just how vulnerable personal data can be and thus what
the motivations might be behind even the most strict data protection
schemes.

IV. SAFE HARBOR PROVISIONS: THE CURRENT COMPROMISE
BETWEEN U.S. AND E.U. INTERESTS

In the wake of the 1995 Directive, the United States Depart-
ment of Commerce worked with the European Union to provide a
way for American companies to comply with the provision that pro-
hibited storage of personal data outside of the geographic boundaries
of the European Union.\textsuperscript{172} The “Safe Harbor,” as it is known, is
comprised of seven principles of E.U. data protection that U.S. com-
panies must comply with in order to be considered “adequate” safe-
guards: (1) Notice, (2) Choice, (3) Onward Transfer, (4) Access, (5)
Security, (6) Data Integrity, and (7) Enforcement.\textsuperscript{173} Fulfilling these
elements is essentially a promise by a company that it will treat data
as if it had never left the European Union and will itself act as if it is
under the E.U.’s jurisdiction.\textsuperscript{174} Notably, the “Choice” element re-

\textsuperscript{168} EPIC—\textit{Investigations of Google Street View}, ELECTRONIC PRIVACY INFORMATION
CENTER, http://epic.org/privacy/streetview/ (last visited March 5, 2013) [hereinafter \textit{Street
View Investigations}].

\textsuperscript{169} \textit{WiFi Data Collection: An Update}, GOOGLE | OFFICIAL BLOG (May 14, 2010) (last
html [hereinafter \textit{WiFi Update}].

\textsuperscript{170} \textit{Street View Investigations}, supra note 168.

\textsuperscript{171} \textit{WiFi Update}, supra note 169.

\textsuperscript{172} 1995 Directive, supra note 99.

\textsuperscript{173} \textit{U.S.-EU Safe Harbor Overview}, EXPORT.GOV (last updated Dec. 18, 2013, 3:45
PM), http://export.gov/safeharbor/ue/eg_main_018476.asp [hereinafter \textit{Safe Harbor
Overview}].

\textsuperscript{174} The passage of the United States PATRIOT Act in 2001 has further complicated
quires allowing a user to be allowed to either affirmatively “opt-in” to the data collection, or to “opt-out” of it, depending on the nature of the information.175

The process for becoming a Safe Harbor is one of self-certification by any company that wishes to participate. As the Department of Commerce informs prospective applicants:

[A]n organization must self-certify annually to the Department of Commerce in writing that it agrees to adhere to the U.S.-EU Safe Harbor Framework’s requirements, which includes elements such as notice, choice, access, and enforcement. It must also state in its published privacy policy statement that it adheres to the Safe Harbor Privacy Principles.176

In other words, companies are given a set of requirements and told to self-certify once a year. A 2000 Department of Commerce Notice claims that the agency dedicated 550 hours and approximately $190,250 to reviewing 1500 Safe Harbor applications, spending twenty minutes per website and forty minutes per letter submitted.177 A 2011 notice of a similar nature cited 343 hours spent for 1,030 applicants, again averaging about twenty minutes per application.178 The FTC and the U.S. Department of Transportation are the bodies responsible for government enforcement of Safe Harbor provisions or prosecutions of violations by American companies if they arise.179

Since its inception in 1998, there have been many criticisms of the Safe Harbor agreement, not the least of which comes from the European Union itself.180 The Commission of the European Com-

---


176. Safe Harbor Overview, supra note 173.


178. Submission for OMB Review; Comment Request, 76 FR 33703-01 (Dept. of Commerce June 9, 2011).


munities published a working document in 2004 that questioned if the FTC was even capable of enforcing the agreement, stating that "the extent to which the FTC has competence to enforce the Safe Harbor Principles regarding human resources data is not clear."181 Furthermore, in the five years after publication of that document, the FTC did not prosecute a single company for violating the Safe Harbor protections to E.U. citizens' privacy.182 We are forced to question why the organization tasked with protecting the privacy of European citizens from American corporations is an American government entity, particularly one that has been sued for not enforcing privacy judgments against those very same companies.183

This question is especially pertinent given the extreme differences between those entities the Americans and the Europeans trust when it comes to their personal data. As the recent National Security Agency (NSA) requests for information have shown, Americans trust corporations more—and their government less—with their personal information compared to Europeans.184 The discrepancy leads to the logical conclusion that the FTC simply cannot adequately protect European privacy interests coming from American corporations.

In short, the Safe Harbor Agreement and its shortcomings throw into sharp relief the different approaches of the United States and the European Union towards privacy. The Agreement also shows both how irreconcilable the two frameworks are with one another and how little progress has been made in that regard since the Safe Harbor was first formed over a decade ago. One author suggests that more transparency regarding the Department of Commerce's review process might help the efficacy of the Agreement but acknowledges that, for any real change to happen, the European Union would likely have to "directly reverse itself and find that the current Safe Harbor protections are not adequate."185 More simply, the European Union could simply enforce the agreement itself, rather than relying on the FTC. While either eventuality is certainly possible in the long

---

181. Id. at 10–11.
182. Leathers, supra note 175, at 195.
183. Supra Part II.B.
185. Leathers, supra note 175, at 222.
run, there has been no indication from either party recently that a re-negotiation of the Safe Harbor Agreement is in the works. For now, both sides are stuck with it, seemingly to the detriment of the European Union.

V. The Great Wall: China’s Protectionist Policies and Privacy Violations

On the one hand, a study of China’s data protection framework with regard to Google is of questionable value, as Google—along with many other non-Chinese companies—has completely withdrawn from the country and currently re-routes any potential users to more secure Hong Kong websites. On the other hand, China represents the world’s biggest internet market with over half a billion users and is the only country so far to force Google to give up its previously unabated attempt to dominate the global internet market. There are several other recent articles that capture the plethora of issues that the Chinese government has created for foreign companies seeking to enter the country—including censorship and human rights issues, protectionist policies, and government-sanctioned hacking/privacy violations—so this discussion will only include a cursory look at their developing policy and interactions with Google.

It is impossible to start any discussion of China’s privacy policies or internet activities without first mentioning the accusations being more and more frequently leveled against the Chinese govern-


189. Liu, supra note 188, at 1204.

190. Id. at 1205-06; see also David Barboza, China’s Internet Giants May Be Stuck There, N.Y. TIMES, Mar. 23, 2010, at B1, available at http://www.nytimes.com/2010/03/24/business/global/24internet.html?_r=0.
mement’s support for state-sponsored hacking.191 Any discussion of data protection rights granted to the citizens—and corporations—of China by the government must be considered against this backdrop of government control, censorship, and, seemingly increasingly, state sponsored invasions of online privacy.192 In fact, it is for precisely these reasons that Google claimed to begin the process that led to its subsequent withdrawal from China in favor of Hong Kong.193 That being said, China does have a developing privacy protection scheme that has recently undergone significant changes that are worth briefly discussing here.194

During the 2010 battle with Google over censorship, the Chinese government amended its Protection of State Secrets Law to include internet companies within the scope of entities required to cooperate with the government to protect state secrets.195 The law served as a better mechanism for China to discover and prosecute dissidents by compelling companies to turn over their data.196 However, in the years since, China experienced an increase in identity theft and online scams to the extent that the government was forced


192. See, e.g., Liu, supra note 188, at 1210 (Chinese government required software—ostensibly to protect children against internet pornography—installed on all computers that recorded user information and sent it back to centralized locations).

193. David Drummond, A New Approach to China, GOOGLE | OFFICIAL BLOG (Jan. 12, 2010), available at http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (Google’s announcement that it had been hacked and would stop censoring results in China).


196. See id.
to seriously consider developing a framework for protecting internet users' personal data—at least from identity thieves and other nongovernmental elements.\footnote{\textit{China Mulls Law for Online Data Protection}, \textsc{Zee News}(Dec. 23, 2012 6:28 PM), available at \url{http://zeenews.india.com/news/world/china-mulls-law-for-online-data-protection_818471.html}.} In fact, in late 2012, a subsection of the Chinese national legislature passed a new set of rules that would make it illegal for individuals or organizations to obtain or misappropriate personal information online and contained a promise that the state would protect information that could identify individuals online.\footnote{\textit{Chinese Legislature Passes Data Privacy Resolution}, \textsc{Hunton Privacy Blog} (Jan. 2, 2013), available at \url{http://www.huntonprivacyblog.com/2013/01/articles/chinese-legislature-passes-data-privacy-resolution/#more-3796}; Leslie A. Pappas, \textit{China Enacts Online Privacy Framework to Protect Data, But Not User Anonymity}, \textsc{Bloomberg BNA} (Jan. 7, 2013), available at \url{http://www.bna.com/china-enacts-online-n17179871719/}.} However, the rules would also require internet users to register their real names in association with their Internet Service Provider Identifications (ISP), a move that could potentially \textit{erode} online privacy.\footnote{\textsuperscript{198} See \textit{Chinese Legislature Passes Data Privacy Resolution}, \textit{supra} note 198.} In addition to the concerns over that part of the law, there are two other factors to consider. First, there neither seems to be an implementation plan for these rules, nor a designated body to enforce them.\footnote{\textsuperscript{200} \textit{Supra} note 198.} Second, while no sufficient translation is yet available to examine the text of the rules, the Chinese government’s past actions indicate that these rules will not protect the personal data of Chinese citizens from the government, which is arguably the biggest threat to a Chinese citizen’s online privacy. Regardless, the legislation represents a possible first step in protecting internet users, albeit a small step measured against several leaps in the other direction. But there has been no indication that such steps will do anything to convince non-domestic companies like Google, Facebook, or Twitter to attempt to re-enter China, and that seems to be just fine with China.

VI. FINDING A BETTER BALANCE: WHAT EACH SCHEME DOES WELL AND WHERE IT MIGHT IMPROVE

Having toured the three vastly different data protection schemes—as well as the attempt to reconcile two of them with each other—it is clear that all three could strike a better balance between safeguarding individual privacy and promoting a welcoming business
environment. This section will make suggestions about how each scheme can be improved both in terms of balance internally and in terms of creating framework more amenable to international corporations and consumers. As discussed above, while diverse privacy norms exist in different societies, this Note’s evaluation of any regulatory scheme will be analyzed—at least in part—based on whether the individual consumer is given the opportunity to give informed consent.

A. United States: Unclear Enforcement Poses Long Term Threat to Both Businesses and Users

With regards to the United States patchwork scheme, there is very little criticism from the business community, although certain polls do show American dissatisfaction with the level of their personal information that is mined by online data collectors.\(^{201}\) Most of the criticism for the United States’ methods of safeguarding personal data comes from legal scholars.\(^{202}\) While there are some scholars that are satisfied with the enforcement and regulation of data protection “on the ground” in the United States,\(^{203}\) there are clear threats to both individual and business interests posed by the lack of a cohesive statutory and enforcement framework. At least one scholar claims that the uncertainty of enforcement stimulates innovation in practice,\(^{204}\) but this stance defies common sense. Without a clear view of what the boundaries of permissible action are, companies are likely more cautious. Evolution of an enforcement policy is one thing, but arguing that an amorphous policy with no clear direction—currently accepted by the United States—actually promotes efficiency is counter-intuitive.

While, at this current moment, the ambiguities in enforcement seem to favor corporations that collect data, states are becoming more active in protecting the personal information of their citizens.\(^{205}\) Without a federal agency authoritatively articulating a central data protection policy, the initiative being taken by state attorneys general could create even more of a patchwork scheme in the United States where corporations will have to tailor their privacy policies to indi-

\(^{201}\) Gallup, supra note 67.
\(^{202}\) Bamberger & Mulligan, supra note 69, at 247.
\(^{203}\) Id. at 311–15.
\(^{204}\) Id. at 307.
\(^{205}\) Supra Part II.B (on state attorneys general becoming more involved in data protection enforcement).
vidual states. Furthermore, the United States’ lax enforcement could arguably be hurting American corporations abroad as the ineffectiveness of the Safe Harbor agreement between the United States and the European Union is largely due to the FTC’s absolute failure to enforce Safe Harbor rules. A reliable replacement for the current Safe Harbor Agreement—or better execution of the existing one—would perhaps decrease the scrutiny that American firms receive upon entering European markets.

On the other hand, the FTC’s failure to enforce even its own decisions shows a failure to protect the personal data of its own citizens as well. If the FTC continues to refuse to embrace its power—and perhaps even push to see just how much power it really has—the American people will truly be left without any sufficient safeguards to protect their personal information. While the most egregious violations—such as Google’s admitted wi-fi grab—will draw attention and subsequent enforcement, corporate self-regulation cannot be expected to sufficiently protect American internet users from “garden variety” attempts at misappropriating their personal information online.

While the FTC acknowledges that this is an era of “rapid change” for data protection, there seems to be a lack of urgency in the United States to create a system that can actually respond to those changes. What remains is an inefficient and cumbersome framework that leaves both corporations and individuals in the dark as to what regulations and protections they can actually expect from the government. While the European statutory framework certainly has its flaws, as discussed below, the United States would be well served by seeking to create a similarly structured system of centralized data protection. This would enable a single agency to establish privacy norms that would benefit corporations and citizens alike.

The agency would be able to establish baseline expectations that internet users would be able to rely on—even as they evolved—and would create an entity better able to specialize and keep up with the rapidly changing landscape of privacy threats on the internet. To the benefit of corporations, this centralized agency would provide a single authority with which companies could interact to develop better policies and provide clear guidelines within which to operate. As for enforcement, giving this hypothetical agency any kind of active mandate for enforcement would provide for a level of protection far beyond anything currently in force. A current U.S. agency that

206. See Guynn, supra note 76.
207. See supra Part III.C.2 (regarding Google Street View cars grabbing data).
comes to mind is the Securities and Exchange Commission (SEC), which has rule-making authority as well as prosecutorial power against offenders.

One concern regarding the SEC analogy is that its enforcement is supplemented by private rights of action by individuals claiming injury. Without proper safeguards against frivolous suits, allowing such a private right of action for alleged data protection violations could lead to a flood of lawsuits that would likely impede companies doing business online. Of course, just as legislation like the Private Security Litigation Reform Act has curtailed frivolous securities actions in the United States, careful legislation could prevent such potential problems.\(^{208}\) Continuing the analogy, securities lawyers have been extremely creative in finding causes of action implied in securities regulations. While the absence of comprehensive legislation has not yet allowed for such ingenuity, it will be interesting to see if future legislation allows for such implied rights of private action. Overall, the SEC analogy is by no means a perfect one, but American internet users and—certainly in the long run—American corporations would benefit from having a specialized rule-making and enforcement agency that oversaw centralized data protection and could authoritatively engage in dialogue with foreign countries to promote cooperation in enforcement.

Until such a regulatory body—or some other kind of check on collectors of personal data—is created, the United States must indeed rely on the market to keep corporations self-regulating honestly, especially in the face of a weak FTC presence. However, further legislation, proposals for which are discussed above,\(^{209}\) need not be sweeping to push privacy protection in the right direction. Rather, any law that requires a website to explicitly ask the user for its permission to record personal information and explains what consent would entail would be a step in the right direction. While such legislation has been derided for being obtrusive to the user experience when passed in Europe, it need not be so heavy-handed to effectively earn the user’s informed consent. It could simply require more extensive public disclosure of privacy practices as well as the specifics of what happens with personal data that is collected. If users know exactly what the products that they use do with their information, the

---


209. See supra Part II.A.
market could actually serve as an adequate protection for consumer privacy under a regime reliant on self-regulation. Furthermore, as discussed above, even marginally more comprehensive legislation could give rise to implied rights of action that would give citizens the ability to protect their own data—or seek recompense for violations of their privacy—through the courts.

B. Europe: Increasing Technical Expertise and Cohesion Among Members

The centralized European framework has drawn criticism from American corporations and technology pundits alike. However, a closer look shows that the criticisms are not aimed at the framework generally, but rather at specific individuals and actions taken that were overly restrictive. In other words, the framework itself—a comprehensive scheme universally derived from a single statute—is logically sound. While the "cookie" directive ordeal elicited harsh criticism, it ultimately showed that the system worked because the process of implementation allowed for discourse that ultimately led to the directive being rendered ineffective. There are two improvements that the European Union could implement in their current system to better promote uniform policies and prevent the criticisms discussed above from continuing.

1. More Technical Expertise in Regulatory Positions

What seem to be lacking in the execution of data protection in the European Union are simply the qualified bodies to occupy these highly technical positions. A quick look at the Working Party—a group stocked with data protection regulators from each E.U. member state—shows a body comprised primarily of career politicians instead of technology or internet professionals. In other words, the criticisms aimed at the E.U. framework seem to be aimed at—and are the result of—not having officials in place who truly understand the intricacies and necessities of online commerce. What is present is the evident desire and force to protect the personal data of E.U. citizens

210. See supra Part III.B (regarding criticism of the cookie directive).

211. Supra Part III.B.

212. This is not to make any commentary on any official’s qualification to hold a position of public trust, but rather the apparent lack of experience in the industry that they are assigned to regulate.

213. Member of the Article 29 Working Party, supra note 116.
from data collecting corporations. Therefore, contrary to what many American critics maintain, I would suggest that the E.U. framework itself is actually in the best position to react to shifting norms as it has a single body that can make decisions and issue advice on how to follow those decisions. After all, the data protection authorities, for all of their harsh words, have been fairly successful in persuading Google to make desired changes without any kind of sanctions or penalties.

To look at the political processes of each E.U. member state to determine exactly how a more tech-friendly Working Party—or individual data protection authority—would be assembled is beyond the scope of this Note. However, the fact remains that recent criticism of the E.U. Cookie Directive or individual data protection authority rulings against Google do not reach the structure of the protection scheme but rather are aimed at specific regulators. The framework as a whole has actually done a good job of addressing the evolving data protection issues head on, if not in the most efficient ways.

2. Better Intra-E.U. Communication Regarding Enforcement

Another way in which the 1995 Directive could be more efficiently executed is to improve communication within the framework’s hierarchy. The current system has allowed multiple data protection authorities to challenge Google or other companies for the same issues.\(^{214}\) This lack of cohesion among the different jurisdictions creates multiple hurdles for corporations where a single regulatory body would likely be sufficient to protect E.U. internet users’ personal data. The repetitive suits represent an obvious inefficiency that deters prospective entrants into the European market and can certainly hinder those that do enter. The two potential remedies that I propose each have their flaws, but show what kind of steps could be taken to alleviate the risk of multiple challenges that each online corporation might potentially face.

The first proposal would be to empower the Working Party (or another separate entity) to enforce all alleged breaches throughout the European Union. This would certainly prevent repetitive challenges by creating a single authority to which each country’s DPA

\(^{214}\) For example, Greece and Germany have both challenged Google Street View. Another example is Google Analytics currently being challenged in Denmark after being cleared by Germany and Norway, a non-E.U. country. There have also been numerous challenges to Google Apps from different countries, both E.U. members and others.
would report violations and entrust to enforce them. Two specific issues with this plan would be (1) that the enforcement agency could be overwhelmed by the sheer number of allegations reported to it, and (2) that countries would be loath to cede enforcement of their own data protection schemes to an outside party. This last effect in particular would likely cause problems in trying to implement such a unified enforcement.

The second proposal would be to allow for a loose, non-binding, precedent-setting system in which any country that ruled on a specific issue could be followed by other E.U. members. For example, under this proposal, whatever Germany’s DPA might have ruled on Google Street View would have also applied to Greece’s complaint. While making such a precedent binding would present the same issue of ceding enforcement power discussed above, the system could be set up more to enhance communication amongst the DPAs of various countries. It could also function to allow a specific DPA to take the lead on privacy issues shared by multiple countries. This practice has already been used at least once when the French data protection agency—the CNIL—took the lead on European concerns over Google’s new privacy policy in early 2012. While seemingly the only instance of such a process, the CNIL’s lead on continent-wide privacy issues shows that the European Union may be headed toward a more cohesive strategy for enforcement among its member states.

Regardless of the criticisms of specific actions, the 1995 Directive created a vehicle that, with the right operators, has the ability to work with corporations to promote business, enforce citizens’ pri-

---

215. To be clear, the European Union is not a federal state that can interfere with any member state’s sovereignty, but rather it is a multi-level governance framework with incredibly complex relationships and few truly powerful regulatory bodies; the European Central Bank is one such example. What I suggest is more an elevated level of communication among E.U. members rather than a precedent-based system in the common law sense.

216. Another possible negative consequence is that such a proposal might create a race to litigate among the countries, with the winner setting a precedent that others must follow. As a result, making the precedent binding would likely do more harm than good to the desired comprehensive regulatory scheme.

vacy rights when corporations overstep their bounds, and present a unified policy to outside nations for the purposes of reconciling different international data protection philosophies. While there are many areas for improvement—noticeably regarding overly restrictive enforcement—the European Union has, at the very least, created a centralized system that can respond to both business and individual concerns over privacy regulations. In fact, the "cookie" directive process showed that it is already doing so, albeit more slowly and inefficiently than corporations would like.

With data protection such a prevalent concern among European citizens, there is promise that the system already in place will continue to adapt to become a more efficient protector of personal data without presenting the hurdles of entry to American corporations that it currently does. However, recent developments show that European lawmakers may simply follow America's lead and soften privacy regulations across the board.218 In light of pressure from American lobbyists, many E.U. legislators were accused of proposing more lenient privacy regulations during reconsideration of the 1995 Directive in June 2013.219 Talks are currently stalled on the European Parliament floor and, while the European Commission denies that there has been a "watering down" of any policies, some legislators have "expressed alarm at the level of lobbying," claiming to have "never seen anything quite like it."220 Of all the possibilities for reform in the European Union, kowtowing to U.S. lobbying interests is one of the least desirable ones from a privacy protection standpoint. As debate continues, there is much to be decided on the course that future privacy regulation will take moving forward.

3. Current Developments

During the writing of this Note, the European Parliament has—under pressure from corporations and privacy watchdogs alike—attempted to reform the 1995 Directive.221 The general belief on both sides of the debate is that the old directive is archaic and out-

219. Id.
220. Id.
dated, but the two sides have been otherwise deadlocked regarding which way to steer the legislation.\footnote{See id.; see also Liat Clark, ICO Commissioner slams EU data protection directive, WIRED (Feb. 07, 2013), http://www.wired.co.uk/news/archive/2013-02/07/ico-against-eu-data-protection.} Privacy watchdogs have pushed for anonymization of personal data, as well as requiring corporations to gain explicit approval from site users to take their personal data, in the form of cookies or otherwise.\footnote{Liat Clark, US data privacy advocates head to Brussels in show of support, WIRED (Jan. 13, 2013), available at http://www.wired.co.uk/news/archive/2013-01/22/us-eu-data-protection-advocates; see also Clark, supra note 222.} On the other hand, American lobbyists have shown up to fight for the interests of Google, Facebook, and other internet companies,\footnote{See Clark, supra note 222.} trying to loosen the European Union’s grip on privacy regulation. As of publication, the two sides are deadlocked with little hope for a resolution in the near future, having tabled any reforms to the 1995 Directive until 2015. This leaves the 1995 Directive as the controlling legislation regarding personal data protection for at least the next year.

C. China: A Long Way to Go

For now, China seems content to exclude foreign companies in favor of their domestic competitors.\footnote{Some examples: Baidu instead of Google Search, Youku and Tudou instead of YouTube, Ren Ren Wang and Kai Xin Wang instead of Facebook, Sina instead of Twitter, Bababian instead of photo-sharing site Flickr. Liu, supra note 188, at 1205–06.} One reason for this is because the government can ensure that domestic companies will work closely with the government to promote and project its political agenda. However, as these companies grow in size—search engine Baidu was the fifth most visited site in the world in 2012\footnote{Alexa Top 500 Global Sites, ALEXA.COM, available at http://www.alexa.com/topsites (last visited March 5, 2013).}—and look to expand, these ties to the Chinese government will potentially slow growth amid suspicion of spying.\footnote{For suspicion of the Chinese government, see Sanger et al., supra note 191.} If China does hope to see these homegrown internet companies gain market traction around the world, it will have to begin to demonstrate that it respects the personal data of its own citizen-users, or at least stop flagrantly attacking foreign companies and governments.

There is no doubt that the legislation passed earlier this year represents a first for the Chinese government, but, to quote the age...
old maxim, "actions speak louder than words." Any laws passed to protect personal data by the legislature will continue to be overshadowed so long as the government continues to have little, if any, regard for anyone's privacy in practice. For now, any company with significant ties to the Chinese government—which is seemingly every Chinese internet corporation—will draw suspicion as the country continues to be accused of government-sponsored hacking of citizens and foreign entities alike. While China is impossible to ignore given the market it presents, it seems to be quite a way from being legitimately included in any attempt to normalize data protection on an international scale.

CONCLUSION

The level of criticism that Google has received has certainly been high; but then again so has the scrutiny, perhaps unfairly so. It is important to note that Google seems to make every possible effort to comply with any legal framework it encounters and the attention that it draws is more from the nature of its success and subsequent growth than any history of malfeasance on the part of the company. This behavior is in contrast to the Chinese government, which publicly states innocence while clear evidence shows a complete lack of regard for data protection. That being said, Google is leading a charge among businesses to monetize the collection of individuals' personal data and online behavioral habits, and that charge is exposing weaknesses in legal protections for citizens everywhere. The growth of the industry is, in fact, making such protections outdated and is doing so at a rate with which it is hard for legislatures to keep pace. Such rapid growth is also keeping consumers increasingly in the dark about what they are giving away, what is being done with that information, and how to protect their privacy online.

In China, the government has taken the unique approach of establishing such control over the internet so as to create totalitarian regime, using the internet to better promulgate its political and social positions. However, this policy has effectively walled off the online economy from foreign data collectors and will likely impede its domestic companies from earning the necessary consumer trust internationally. While recent legislation represents token steps taken towards individual data protection, until the Chinese government shows a real willingness to respect the privacy of individuals, let alone foreign corporations and governments, it will not have a place at the table for the global discussion on data protection.

In terms of that global discussion, this Note highlights some
of the many problems that a single regulatory framework can encounter when being faced with a rapidly changing industry. The E.U.'s two year "cookie" directive debacle certainly highlights how an out-of-touch legislature, comprised of people with little industry experience, can create unnecessary hurdles for internet businesses and users alike. However, it also shows how a single, powerful agency that seemingly reflects its citizens' commitment to personal privacy can force an industry to take a closer look at its activities, even without any serious sanctions. That the process of regulation laid out by the 1995 Directive effectively removed the teeth of the "cookie" directive shows that the process could actually work, although it will certainly continue to draw the ire of internet corporations and their supporters. If the Working Party and national data protection authorities can begin to include more industry leaders—either through collaboration or direct inclusion as regulators—then the E.U. data protection framework could become a model for balancing privacy with economic interests in a global market. However, that is easier said than done, and involving industry leaders too much can result in lobbying interests taking control of future privacy regulation in Europe.

As for the American framework, Congress seems committed to avoiding comprehensive legislation nearly as much as the FTC seems loathe to flexing its regulatory muscle. While a general distrust of such data collection practices seems to exist among polled Americans, the only real outcry for any change to the current framework is currently coming from scholars and privacy advocates. Still, as the information gap between consumers and the corporations that are tracking them grows, concerns about the continued efficacy of self-regulation in an uninformed market are on the mark, to say the least.

Given that the vast majority of the most visited and valuable internet companies in the world have grown under such a framework, it is hard to imagine the United States changing course so drastically as to adopt a single legislative framework to govern all data protection. However, the FTC's failure to enforce anything but the most egregious privacy violations creates a regulatory void that the United States should seriously discuss filling. The uncertainty created by the combination of an unclear legislative framework and inconsistent regulation—one that is allowing for such innovation and development on the corporate side right now—does not seem sustainable; especially in light of privacy advocates' concerns that, once lost, personal privacy online will be nearly impossible to reclaim. While the U.S. framework has drawn the least criticism of the regimes discussed in this Note, and has produced some of the world's most dominant internet companies, it also is cause for serious concerns about
personal data in the future.

In an era that the FTC has correctly dubbed one of "rapid change," the lag in data protection enforcement is understandable. Individuals are only just now beginning to realize that the free products they use online are potentially paid for with their personal information, and that concern inevitably takes some time to make it into the legislature. The role of governments in protecting the privacy of their people, while not universal—see China—seems to be shared between the United States and Europe. However, the two differ on what is the best method for balancing that right to privacy with economic interests and online business development. Moving forward, both frameworks must focus not only on better internal regulations as discussed above, but also on creating a better dialogue between the two regimes. The internet economy is a global one, and data collection is going to happen to all internet users by an increasing number of corporations around the world. The sooner a better dialogue begins, the sooner these governments can start to catch up to the ever-growing list of privacy challenges facing today's internet user in what is truly an era of rapid change.

John Schinasi*

* Executive Editor, Columbia Journal of Transnational Law; J.D. Candidate, Columbia Law School, 2014; B.A. University of Michigan, 2007. The author would like to thank Professor Katharina Pistor for her guidance—and patience with him—throughout the research and writing process. He is also grateful to Ryan for the many long discussions that sparked his interest in this subject. Additionally, the author owes a debt of thanks to all of the Journal staffers and editors who worked hard to make this Note publishable. Finally, to his parents, Katherine and Garry: the author wishes to convey his eternal gratitude for their constant love, support, and guidance.