

**The Future of Privacy Forum**

**News in Review**

# FPF Quick Clips

# “Even Without Legislation, Privacy Will Be a Hot Issue in 2012” Jules Polonetsky, Omer Tene and Christopher Wolf, National Journal, January 5, 2012

#  “Privacy concerns and technological change: the legislative option” Jules Polonetsky and Christopher Wolf, The Hill’s Congress Blog, January 31, 2012

# “Privacy in the Year of Big Data: A Time for Big Decisions” Jules Polonetsky and Omer Tene, Stanford Law Review, February 2, 2012

# “The Growing Problem of Privacy-Invading Mobile Apps” Jules Polonetsky and Christopher Wolf, Forbes, February 23, 2012

# “Jules Polonetsky and Christopher Wolf: App developers, not regulators, are best suited to solve privacy problem” San Jose Mercury News, March 19, 2012

# “U.S. Senate is Considering a TMI Law”, Christopher Wolf, San Francisco Chronicle, April 16, 2012

# “Why They Track Us” Jules Polonetsky and Christopher Wolf, Huffington Post Technology, May 3, 2012

# “Privacy: Light Slap For Dharun Ravi; Big Penalties For Dot-Coms” Christopher Wolf, Forbes, June 1, 2012

# “Encryption and Globalization” Peter Swire and Kenesa Ahmad, Columbia Science and Technology Law Review (forthcoming 2012)

*QUICK CLIPS*

**

**

*“It’s time for app developers to take responsibility for ensuring that users know what they’re doing, rather than leaving it to the platforms to play a game of Whac-A-Mole,” said Jules Polonetsky, director of the Future of Privacy Forum.*

**

**

*Chris Wolf, the co-chair of the Future of Privacy Forum, echoed those comments, saying this is a “co-regulation” model, and one that he believes will help the U.S. address privacy in an era of changing technological innovation. In a statement, Wolf said he hopes lawmakers in Europe will look to this same model as a potential one for regulation.*





*They're still not going to read it," said Jules Polonetsky, director of the Future of Privacy Forum.*

 *He added that posting broad privacy policies is still important, even if consumers don't read them. It forces companies to carefully consider how they use information, provides standards that regulators can hold them to and allows privacy wonks and tech writers to read and highlight the critical points.*

**

**

*Jules Polonetsky, director and co-chair of the Future of Privacy Forum, commended the attorney general for brokering the agreement.*

 *“Apps can only provide innovative services to consumers if they use personal information responsibly,” Polonetsky said. “If apps surprise consumers by grabbing information that isn’t needed or by surprising consumers, they risk losing access to user data. The California agreement will ensure that consumers are protected and that the app environment continues to flourish.”*

**

**

*“For many people, automatic sharing and social media is how they shape their online identities,” Wolf said.*

**

*"It is gratifying to see that the input provided by the Future of Privacy Forum was useful to the FTC, which repeatedly cites the Forum in the Report," said Christopher Wolf, co-chair of the Future of Privacy Forum. "The FTC's definition of the scope of privacy protection is flexible and sensible, and allows for use of de-identified data.*

**

**

*“I think there are a lot of companies that have been concerned by the recent litigation and constant criticism who see this as an opportunity to be at the table and help shape solutions,” says Jules Polonetsky, director of the Future of Privacy Forum and former chief privacy officer of DoubleClick.*

*“I’m optimistic that there will be enough major players cooperating that we’ll see real successes in a few key areas,” says Polonetsky. “If we try to solve all of the privacy issues for the whole industry, we’ll probably be arguing for the next 50 years.”*





While few expect Congress to pass broad privacy legislation, privacy will still get a lot of attention in 2012, starting with the release in the coming weeks of two highly anticipated federal reports providing guidance on protecting consumer privacy online.

Both the Commerce Department and the Federal Trade Commission are set to release separate final reports with recommendations on how to improve online privacy.

Commerce, which could release its final report the last week of January, will outline the Obama administration’s policy on the issue. Since issuing its draft report in December 2010, the administration has called on Congress to pass legislation that would provide consumers with privacy protections based on the Fair Information Practice Principles embraced by many countries. These include providing consumers with notice about the information being collected about them, choice, access to the information, and security to ensure the data is protected.

In its draft staff report, also released in December 2010, the FTC did not call on Congress to pass privacy legislation but it did come out in support of a system that would give consumers a choice on whether they want to be tracked online. During a briefing on Thursday sponsored by Microsoft, Maneesha Mithal with the FTC’ s Bureau of Consumer Protection said the commission is aiming to release its final privacy report in the coming weeks. She and other FTC officials, however, have so far declined to provide many details of the report.

During a separate event on Thursday focused on privacy issues that may emerge this year, **Jules Polonetsky**, director of the Future of Privacy Forum, said he expects the FTC will likely come out in support of an industry self-regulatory program that allows consumers to click on an icon and opt out of receiving ads based on information collected by tracking their online habits. In its draft staff report, the FTC said that efforts by industry to regulate themselves on privacy had been inadequate.

The Commerce Department report could come out days before the European Commission releases its proposed changes to its privacy directive, which could affect U.S. companies that do business in Europe or operate websites used by Europeans. The commission is expected to call for making the directive a regulation to be imposed on its member states.

In addition, the commission is expected to call for increasing fines, requiring express consent from consumers before collecting information about them, and expanding the scope of the privacy law to include websites targeting EU citizens and not just those companies with European operations. “It’s evident it's taking a rather heavy-handed strict regulatory approach,” said **Omer Tene**, a senior fellow with the Future of Privacy Forum and a visiting fellow at the Berkeley Center for Law and Technology.

Because the United States does not have a broad privacy law, U.S. companies have managed to comply with the EU privacy directive through a safe-harbor agreement with the European Union. But Future of Privacy Forum Cochairman **Christopher Wolf** said the EU may reevaluate that agreement in light of the proposed changes to its privacy directive. Some privacy advocates have argued that the EU’s changes may ultimately force the United States to bolster its privacy protections.

Despite this, Wolf and others say it’s unlikely Congress will pass privacy legislation this year. And while committees in both chambers held several hearings last year, Wolf said lawmakers will use their oversight authority to hold more hearings this year on various privacy issues, which can prompt voluntary action by companies.

“In an election year in what can charitably be called a dysfunctional Congress, the odds are against any privacy legislation becoming law in 2012,” Wolf said.

******

**

In the recent Supreme Court case where all nine justices agreed that placing a GPS tracking device on a car without a warrant violated the Fourth Amendment, Justice Alito observed that "in circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." But since there was no GPS tracking device law for guidance, Justice Alito and his colleagues looked to Fourth Amendment precedent to analyze warrantless use of the new(ish) GPS technology and to create a privacy solution. Henceforth, as a matter of Constitutional law, police need a warrant before they attach a GPS tracking device to someone's car. The Supreme Court came up with the right result even without a specific statute.

Justice Alito is not alone in thinking that privacy legislation is the best way to deal with technological change. Last year, dozens of bills were introduced in Congress to regulate online tracking, to create rules for the collection of geolocation data, to protect children's privacy and to regulate the collection and use of personal data generally. None were passed, but attention to privacy issues reached a new high and included a series of high-profile Congressional

hearings.

Recently, the Obama Administration finalized its study of privacy issues and called for the passage of a consumer legislation which it dubbed a "Privacy Bill of Rights." And across the Atlantic, the European Commission unveiled a proposal for a EU-wide regulation to replace the current privacy law framework, with very specific restrictions and very significant penalties for non-compliance.

Do all of these proposals for new laws confirm Justice Alito's dictum that with "dramatic technological change, the best solution to privacy concerns" is legislative? Maybe, but the answer depends on what kind of legislation.

Many believe that the proposals coming from Europe are too detailed, too strict and too draconian, with the result that technological innovation will suffer. And on both sides of the Atlantic, technology advances much faster than laws can be drafted, compromised and passed. Moreover, technology-specific laws may be outmoded as soon as they come into force. Congress is grappling right now with an electronic privacy law passed in the 1980s that never contemplated e-mail or cloud computing, but nevertheless is the only law dealing with government access to our remotely-stored data. And a privacy law intended to address video rental stores sharing customer records (passed at a time when streaming online video was not on the horizon) has created the perverse situation under which Facebook users can freely share with their friends what music they are streaming from online services but cannot easily share the videos they are streaming from Netflix.

The Administration's legislative proposal contemplates a Safe Harbor for companies that participate in enforceable privacy codes of conduct approved by the Federal Trade Commission, thereby allowing the codes to be flexible and nimble as technology evolves. Meanwhile, great strides in privacy protection already have been made through industry efforts to do better. Last year, there was intense scrutiny of online tracking to deliver targeted advertising -- the so-called "Do Not Track" issue. This year, we see browser controls for online tracking, dashboard for consumers to make tracking choices and catchy icons appended to online ads that can be clicked through for more information and control over tracking. The right result, even without a specific statute.

New privacy issues are raised each week. The latest controversy is over changes to the Google privacy policy. The existing privacy framework is available to deal with that, especially since Google is under the FTC's jurisdiction. No new legislation is needed for every controversy du jour.

Smart privacy legislation is legislation that flexibly covers changes in technology, that does not stifle innovation and that promotes industry-initiated progress in coming up with privacy solutions. Surely that is the kind of guiding legislation Justice Alito, and privacy advocates, would appreciate.



Privacy in the Age of Big Data

A Time for Big Decisions

[PDF](http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf) [Print](http://www.stanfordlawreview.org/printer-friendly/printer-friendly/online/privacy-paradox/big-data) [Author Bios on the Future of Privacy Forum](http://www.futureofprivacy.org/category/the-team/)

February 2, 2012 64 Stan. L. Rev. Online 63

**By Omer Tene & Jules Polonetsky**

*Omer Tene is an Associate Professor at the College of Management Haim Striks School of Law
Jules Polonetsky is a Co-Chair and Director of the Future of Privacy Forum*

We live in an age of “big data.” Data has become the raw material of production, a new source of immense economic and social value. Advances in data mining and analytics and the massive increase in computing power and data storage capacity have expanded, by orders of magnitude, the scope of information available to businesses, government, and individuals.[**[1]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_1) In addition, the increasing number of people, devices, and sensors that are now connected by digital networks has revolutionized the ability to generate, communicate, share, and access data.[**[2]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_2) Data create enormous value for the global economy, driving innovation, productivity, efficiency, and growth. At the same time, the “data deluge” presents privacy concerns that could stir a regulatory backlash, dampening the data economy and stifling innovation.[**[3]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_3) In order to craft a balance between beneficial uses of data and the protection of individual privacy, policymakers must address some of the most fundamental concepts of privacy law, including the definition of “personally identifiable information,” the role of consent, and the principles of purpose limitation and data minimization.

Big Data: Big Benefits

The uses of big data can be transformative, and the possible uses of the data can be difficult to anticipate at the time of initial collection. For example, the discovery of Vioxx’s adverse effects, which led to its withdrawal from the market, was made possible by the analysis of clinical and cost data collected by Kaiser Permanente, a California-based managed-care consortium. Had Kaiser Permanente not connected these clinical and cost data, researchers might not have been able to attribute 27,000 cardiac arrest deaths occurring between 1999 and 2003 to use of Vioxx.[**[4]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_4) Another oft-cited example is Google Flu Trends, a service that predicts and locates outbreaks of the flu by making use of information—aggregate search queries—not originally collected with this innovative application in mind.[**[5]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_5) Of course, early detection of disease, when followed by rapid response, can reduce the impact of both seasonal and pandemic influenza.

While a significant driver for research and innovation, the health sector is by no means the only arena for transformative data use. Another example is the “smart grid,” which refers to the modernization of the current electrical grid to achieve a bidirectional flow of information and electricity. The smart grid is designed to allow electricity service providers, users, and other third parties to monitor and control electricity use. Some of the benefits accrue directly to consumers, who are able to reduce energy consumption by learning which devices and appliances consume the most energy, or which times of the day put the highest or lowest overall demand on the grid. Other benefits, such as accurately predicting energy demands to optimize renewable sources, are reaped by society at large.

Traffic management and control is another field witnessing significant data-driven environmental innovation. Governments around the world are establishing electronic toll pricing systems, which set forth differentiated payments based on mobility and congestion charges. Users pay depending on their use of vehicles and roads. These and other uses of data for traffic control enable governments to “potentially cut congestion and the emission of pollutants.”[**[6]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_6)

Big data is also transforming the retail market. Indeed, Wal-Mart’s inventory-management system, called Retail Link, pioneered the age of big data by enabling suppliers to see the exact number of their products on every shelf of every store at each precise moment in time. Many of us use Amazon’s “Customers Who Bought This Also Bought” feature, prompting users to consider buying additional items selected by a collaborative filtering tool. Analytics can likewise be used in the offline environment to study customers’ in-store behavior in order to improve store layout, product mix, and shelf positioning.

Big Data: Big Concerns

The harvesting of large data sets and the use of analytics clearly implicate privacy concerns. The tasks of ensuring data security and protecting privacy become harder as information is multiplied and shared ever more widely around the world. Information regarding individuals’ health, location, electricity use, and online activity is exposed to scrutiny, raising concerns about profiling, discrimination, exclusion, and loss of control. Traditionally, organizations used various methods of de-identification (anonymization, pseudonymization, encryption, key-coding, data sharding) to distance data from real identities and allow analysis to proceed while at the same time containing privacy concerns. Over the past few years, however, computer scientists have repeatedly shown that even anonymized data can often be re-identified and attributed to specific individuals.[**[7]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_7) In an influential law review article, Paul Ohm observed that “[r]eidentification science disrupts the privacy policy landscape by undermining the faith that we have placed in anonymization.”[**[8]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_8) The implications for government and businesses can be stark, given that de-identification has become a key component of numerous business models, most notably in the contexts of health data (regarding clinical trials, for example), online behavioral advertising, and cloud computing.

What Data is “Personal?”

We urge caution, however, when drawing conclusions from the re-identification debate. One possible conclusion, apparently supported by Ohm himself, is that all data should be treated as personally identifiable and subjected to the regulatory framework.[**[9]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_9) Yet such a result would create perverse incentives for organizations to abandon de-identification and therefore increase, rather than alleviate, privacy and data security risks.[**[10]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_10) A further pitfall is that with a vastly expanded definition of personally identifiable information, the privacy and data protection framework would become all but unworkable. The current framework, which is difficult enough to comply with and enforce in its existing scope, may well become unmanageable if it extends to any piece of information. Moreover, as Betsy Masiello and Alma Whitten have noted, while

*[a]nonym[ized] information will always carry some risk of re-identification . . . . [m]any of the most pressing privacy risks . . . exist only if there is certainty in re-identification, that is if the information can be authenticated. As uncertainty is introduced into the re-identification equation, we cannot know that the information truly corresponds to a particular individual; it becomes more anonymous as larger amounts of uncertainty are introduced.*[***[11]***](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_11)

Most importantly, if information that is not ostensibly about individuals comes under full remit of privacy laws based on a possibility of it being linked to an individual at some point in time through some conceivable method, no matter how unlikely to be used, many beneficial uses of data would be severely curtailed. Such an approach presumes that a value judgment has been made in favor of individual control over highly beneficial uses of data, but it is doubtful that such a value choice *has* consciously been made. Thus, the seemingly technical discussion concerning the scope of information viewed as personally identifiable masks a fundamental normative question. Policymakers should engage with this normative question, consider which activities are socially acceptable, and spell out the default norms accordingly. In doing so, they should assess the value of data uses against potential privacy risks, examine the practicability of obtaining true and informed consent, and keep in mind the enforceability of restrictions on data flows.

Opt-in or Opt-out?

Privacy and data protection laws are premised on individual control over information and on principles such as data minimization and purpose limitation. Yet it is not clear that minimizing information collection is always a practical approach to privacy in the age of big data. The principles of privacy and data protection must be balanced against additional societal values such as public health, national security and law enforcement, environmental protection, and economic efficiency. A coherent framework would be based on a risk matrix, taking into account the value of different uses of data against the potential risks to individual autonomy and privacy. Where the benefits of prospective data use clearly outweigh privacy risks, the legitimacy of processing should be assumed even if individuals decline to consent. For example, web analytics—the measurement, collection, analysis, and reporting of internet data for purposes of understanding and optimizing web usage—creates rich value by ensuring that products and services can be improved to better serve consumers. Privacy risks are minimal, since analytics, if properly implemented, deals with statistical data, typically in de-identified form. Yet requiring online users to opt into analytics would no doubt severely curtail its application and use.

Policymakers must also address the role of consent in the privacy framework.[**[12]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_12) Currently, too many processing activities are premised on individual consent. Yet individuals are ill-placed to make responsible decisions about their personal data given, on the one hand, well-documented cognitive biases, and on the other hand the increasing complexity of the information ecosystem. For example, Alessandro Acquisti and his colleagues have shown that, simply by providing users a *feeling* of control, businesses encourage the sharing of data, regardless of whether or not a user has actually gained control.[**[13]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_13) Joseph Turow and others have shown that “[w]hen consumers see the term ‘privacy policy,’ they believe that their personal information will be protected in specific ways; in particular, they assume that a website that advertises a privacy policy will not share their personal information.”[**[14]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_14) In reality, however, “this is not the case.”[**[15]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_15) Privacy policies often serve more as liability disclaimers for businesses than as assurances of privacy for consumers.

At the same time, collective action problems may generate a suboptimal equilibrium where individuals fail to opt into societally beneficial data processing in the hope of free riding on the goodwill of their peers. Consider, for example, internet browser crash reports, which very few users opt into, not so much because of real privacy concerns but rather due to a (misplaced) belief that others will do so instead. This phenomenon is evident in other contexts where the difference between opt-in and opt-out regimes is unambiguous, such as organ donation rates. In countries where organ donation is opt-in, donation rates tend to be very low compared to the rates in countries that are culturally similar but have an opt-out regime.[**[16]**](http://www.stanfordlawreview.org/printer-friendly/online/privacy-paradox/big-data#footnote_16) Finally, a consent-based regulatory model tends to be regressive, since individuals’ expectations are based on existing perceptions. For example, if Facebook had not proactively launched its News Feed feature in 2006 and had instead waited for users to opt-in, we might not have benefitted from Facebook as we know it today. It was only after data started flowing that users became accustomed to the change.

We do not argue that individuals should *never* be asked to expressly authorize the use of their information or offered an option to opt out. Certainly, for many types of data collection and use, such as in the contexts of direct marketing, behavioral advertising, third-party data brokering, or location-based services, consent should be solicited or opt-out granted. But an increasing focus on express consent and data minimization, with little appreciation for the value of uses for data, could jeopardize innovation and beneficial societal advances. The question of the legitimacy of data use has always been intended to take into account additional values beyond privacy, as seen in the example of law enforcement, which has traditionally been allotted a degree of freedom to override privacy restrictions.

Conclusion

Privacy advocates and data regulators increasingly decry the era of big data as they observe the growing ubiquity of data collection and the increasingly robust uses of data enabled by powerful processors and unlimited storage. Researchers, businesses, and entrepreneurs vehemently point to concrete or anticipated innovations that may be dependent on the default collection of large data sets. We call for the development of a model where the benefits of data for businesses and researchers are balanced against individual privacy rights. Such a model would help determine whether processing can be justified based on legitimate business interest or only subject to individual consent, and whether consent must be structured as opt-in or opt-out.

1. See, e.g., Kenneth Cukier, Data, Data Everywhere, Economist, Feb. 27, 2010, at 3-5, available at http://www.economist.com/node/15557443.
2. See, e.g., Omer Tene, Privacy: The New Generations, 1 Int’l Data Privacy Law 15 (2011), available at <http://idpl.oxfordjournals.org/content/1/1/15.full>.
3. Consider, for example, the draft Regulation proposed on January 25, 2012, by the European Commission to replace the 1995 Data Protection Directive. It is poised to significantly increase sanctions, expand the geographical scope of the law, tighten requirements for explicit consent, and introduce a new “right to be forgotten.” See Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012), available at <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>.
4. Rita Rubin, How Did Vioxx Debacle Happen?, USA Today, Oct. 12, 2004, at D1, available at http://www.usatoday.com/news/health/2004-10-12-vioxx-cover\_x.htm.
5. See Google Flu Trends: How Does This Work?, Google, <http://www.google.org/flutrends/about/how.html> (last visited Jan. 25, 2012). Also consider Google Translate, which provides a free and highly useful statistical machine translation service capable of translating between roughly sixty languages by relying on algorithms and data freely available on the Web. See Inside Google Translate, Google, <http://translate.google.com/about/intl/en_ALL/> (last visited Jan. 25, 2012).
6. McKinsey Global Inst., Big Data: The Next Frontier for Innovation, Competition, and Productivity 91-92 (2011), available at <http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation>.
7. This line of research was pioneered by Latanya Sweeney and made accessible to lawyers by Paul Ohm. See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010); Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, 2008 Proc. of IEEE Symp. on Security & Privacy 111; Latanya Sweeney, Simple Demographics Often Identify People Uniquely 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000).
8. Ohm, supra note 7, at 1704.
9. See id. at 1742-43.
10. Ann Cavoukian & Khaled El Emam, Info. & Privacy Comm’r of Ont., Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy 7 (2011), available at <http://www.ipc.on.ca/images/Resources/anonymization.pdf>.
11. Betsy Masiello & Alma Whitten, Engineering Privacy in an Age of Information Abundance, 2010 AAAI Spring Symp. Series 119, 122, available at <http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/viewFile/1188/1497>; see also Cynthia Dwork, Differential Privacy, 2006 Int’l Colloquium on Automata, Languages and Programming pt. II, at 8, available at <http://www.dbis.informatik.hu-berlin.de/fileadmin/lectures/SS2011/VL_Privacy/Differential_Privacy.pdf> (introducing the concept of a privacy-preserving statistical database, which enables users to learn properties of a population while protecting the privacy of individuals).
12. See, in a different context, Omer Tene & Jules Polonetsky, To Track or ‘Do Not Track’: Advancing Transparency and Individual Control in Online Behavioral Advertising, 13 Minn. J. L. Sci. & Tech. (forthcoming 2012) (arguing that “[i]n the context of online privacy . . . emphasis should be placed less on notice and choice and more on implementing policy decisions with respect to the utility of given business practices and on organizational compliance with fair information principles”). See also Nicklas Lundblad & Betsy Masiello, Opt-in Dystopias, 7 SCRIPTed 155, 155 (2010), [http://www.law.ed.ac.uk/ahrc/scripted/vol7-1/lundblad.asp](http://www.law.ed.ac.uk/ahrc/scripted/) (contending that while “[o]pt-in appears to be the optimal solution for anyone who believes consumers should have choice and control over their personal data collection… upon closer examination, it becomes clear that opt-in is a rhetorical straw-man that cannot really be implemented by regulatory policies without creating a number of unintended side effects, many of which are suboptimal for individual privacy”).
13. Laura Brandimarte, Alessandro Acquisti & George Loewenstein, Misplaced Confidences: Privacy and the Control Paradox, (Sept. 2010) (unpublished manuscript), available at <http://www.futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf>.
14. Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good & Jens Grossklags, The Federal Trade Commission and Consumer Privacy in the Coming Decade, 3(3) I/S: J. L. & Pol’y for Info. Soc’y 723, 724 (2007).
15. Id.
16. Consider, for example, the donation rates in Sweden (opt-out) and Denmark (opt-in), 85.9% and 4.25% respectively; or in Austria (opt-out) and Germany (opt-in), 99.9% and 12% respectively. Notice, however, that additional factors besides individuals’ willingness to participate, such as funding and regional organization, affect the ultimate conversion rate for organ transplants. Eric J. Johnson & Daniel Goldstein, Do Defaults Save Lives?, 302 Science 1338 (2003).

******

**The Growing Problem of Privacy-Invading Mobile Apps**

**

*February 23, 2012*

Mobile device apps are all the rage. But now, people are all *enraged* over the news that some apps accessed and uploaded the contents of user address books without permission. The developers of the apps do not appear to be bad guys. They weren’t selling the information to spammers or using the information for marketing purposes. They thought it was a good idea to upload the address books to help users connect with friends who use the same app.

But it was a really bad idea. In taking personal information without permission, users felt violated and powerless. The problem is compounded by the apparent poor security for the data that was taken.

Unfortunately, taking personal information without basic privacy protections is not an isolated problem. Our recent survey of the most popular apps showed that basics like a privacy policy were missing for a shocking number of apps. Many app developers don’t seem to be aware of the importance of ensuring users understand how data is going to be used. And ignorance of privacy can be a big problem, because apps can access a wide range of personal data – just about anything stored on a mobile device. Far too many app developers have not taken the time to get privacy right.

Why not? There are lots of excuses: “We are just a start-up,” or “too many privacy rules will get in the way of cool app functions.” And so on.

The stakes for the future of the app ecosystem are high. Apps using personal data can provide a range of user benefits, but accessing user data is a privilege, not a right. To ensure access to useful data on mobile devices, developers need to make user trust their first priority. If users are worried about what apps do with their data, there will be no trust. And without trust, app developers may find that users or app store platforms will lock down the data.

Some are looking to Apple and Google to make their app platforms responsible for the privacy practices of the hundreds of thousands of apps on the market. They and other platforms do have a key role to play in setting basic privacy rules for developers who use their app stores. In fact, the terms of service for developers in both leading app stores already restrict developers from loading information, such as an address book, without notification. Clearly far more needs to be done to educate developers about the rules of the road.

But there is no conceivable way that the platforms will be able to police the activities of what in a few years= will be millions of apps across platforms that will cross phones, desktops, smart TVs, smart home systems and more. Do we want one or two companies to be gatekeepers of every program we use? We need the platforms setting a baseline of privacy and security norms, but we need to get the balance right to ensure consumer choice and continued innovation.

The government is already stepping in to the fray. The Federal Trade Commission this week told app developers that target children that they will be the first priority for upcoming enforcement activity. Members of Congress have held hearings and class action lawyers have already filed lawsuits against developers and platforms. The new generation of app developers doesn’t have time to spare.

The rest of us can help by doing our part. Companies like PrivacyChoice and TRUSTe already provide developers with privacy tools. The Future of Privacy Forum hosts a privacy education site designed especially for app developers and has partnered with the App Developers Alliance for an upcoming privacy summit in San Francisco. A number of trade groups already have proposed best practices for developers. The privacy community needs to expand its efforts to target app developers for awareness-raising and training.

Communication to users about privacy on a small mobile device isn’t easy, and app developers often are limited by technology or platform limitations when they want to provide users with information. Users aren’t delighted by the legalese they see in long desktop policies, so it’s not like we have all the answers for the new mobile issues. If app developers bring the same creativity to mobile privacy that they have to launching new services, they may solve their own problems and teach the rest of us something new as well. Privacy could use a healthy dose of innovation right about now.

**

****

For years, marketers dreamed of the day when smartphones would be ubiquitous. Users would get ads based on their actual location at the time. Offers would be delivered right to the consumer's pocket. All agreed that privacy and user permission would be sacred because, after all, this was very sensitive data. Users considered their phones to be a highly personal device. Overstepping boundaries would not be tolerated.

So how are things working out?

Smartphones are indeed ubiquitous. The personal data available far outstrips what was ever imagined. Location, address books, social network relationships, photos, texts, emails and other highly personal information is stored on these devices and many users feel so tied to their phones that they keep them in reach even when in bed.

Unfortunately, it seems that just about every week we hear about another example of mobile misbehavior. Leading mobile apps are caught uploading users' address books without bothering to ask. iPhone and Android phones are accused of allowing apps to access users' photos without clear permission. Advertising companies are using technical tricks to bypass mobile browser privacy settings. Our recent Future of Privacy Forum survey showed that only a third of the most popular apps even bothered to have a privacy policy.

What has gone wrong?

To some extent, the mobile ecosystem is a victim of its own success. Several years ago, regulated cellphone carriers provided network service, sold phones and decided what apps could be made available. Today, the mobile smartphone environment is a fast-growing, chaotic system of platforms provided by Apple or Google, independent app developers, mobile ad networks and other third parties. Hundreds of thousands of developers provide innovative new features using the personal data they access on consumer devices, many with little experience managing the giant databases they can assemble.

Each misstep leads to an explosion of tweets, blog posts and complaints. If companies don't get their acts together quickly, users may stop feeling so free about sharing the data that has been the driver of new services and profits.

Thankfully, some progress is being made. California Attorney General Kamala Harris recently entered into an agreement with six leading app store and platform operators that will allow consumers to review an app's privacy policy before they download the app. The agreement also commits platforms to educate developers about their obligations to respect consumer data. The platforms will work to improve compliance with privacy laws by giving users tools to report noncompliant apps and committing companies to responding to these reports.

Similarly, the Federal Trade Commission has put developers on notice that it is ready to take action against apps that are acting deceptively. And the Obama administration is signaling that mobile apps may be the first sector it seeks to convene for a multi-stakeholder effort to develop enforceable privacy guidelines.

We welcome the policy-makers into the fray and are advancing the dialogue by hosting an app developer privacy summit to bring together developers, platforms and government regulators in San Francisco. But the folks best suited to solve the problem are the app developers themselves.

The energy and ingenuity displayed by the venture and developer communities in creating and launching apps can address consumer concerns far more effectively than the government. Don't wait for us to tell you what to do. Show up with solutions in hand. Just remember that access to user data is a privilege, not a right. Now start coding!



**

Should Congress be in the business of deciding what people can share through social media? That is the question considered at one of only three hearings so far by the Senate Judiciary Privacy Subcommittee. The three senators at the hearing each suggested that without legal restrictions, people might over-share information about what streaming videos they watch online. That is, the senators are worried about TMI - too much information.

For some, regular sharing is TMI. For others, it is part of proactively shaping their online identities and an essential way to spread their ideas. Social media provides a wonderful opportunity for free expression and connection, but users need to be sensitive of the risks of TMI. In short, we need cyber-education, parental guidance and self-editing. But do we need a federal law limiting how much users share about their online movie watching?

The Senate Judiciary Privacy Subcommittee took up the issue as part of its review of the 1988 Video Privacy Protection Act. The act was passed in reaction to a newspaper reporter obtaining the video rental records of then-Supreme Court nominee Judge Robert Bork, and it restricts sharing rental records without a person's permission. Some read that law though as to prevent the use of automatic sharing tools that many Facebook users employ to share the music they listen to on the streaming music service Spotify, or the news articles they read on the Washington Post online. That reading of the law has inhibited the launch of a Netflix "frictionless" sharing tool, and there are calls for an amendment to the act to specify that frictionless sharing is illegal.

Netflix is not the only online streaming video service whose users may be foreclosed from sharing their viewing experiences. Amazon, Blockbuster, Hulu and Vudu offer streaming video services and their users (and those of services yet to be launched) also stand to be affected by a law that prohibits consumers from choosing to share their online viewing choices.

Advocates of restrictions on frictionless sharing are concerned that Facebook users might inadvertently disclose through the automatic sharing tool that they watched a controversial movie, causing personal embarrassment. They propose that, as to movies only and as a matter of law, users must choose on a case-by-case basis what movies they want to post on Facebook.

At a recent hearing, Sen. Al Franken referenced the movie, "The Godfather." Using his example, if I read an electronic version of the book and want to use a feature that automatically posts that fact to my Facebook page, that's fine. But if I watch the movie online, I would be prohibited by law from automatically sharing that with my friends on Facebook.

A law limiting the ability of people to choose to share all of the movies they watch online is not what privacy law should be about. Privacy is about empowering individuals with the ability to choose what information they want to disclose, and to whom. It is not the business of privacy law to decide.

A House amendment to the act would allow movie watchers to share the movies they are streaming so long as the choice provided is "opt in," not "opt out" with sharing as a default, and so long as the sharing choice is prominent and separated from the standard privacy and website terms.

Of course, not everyone wants to share their viewing experiences with their friends online, and they don't have to share. And if someone prefers to share their video watching experiences on a case-by-case basis, he or she can do so manually. Similarly, a person who chooses to share on a continuous basis can disable the share function before watching a streaming video that he or she wants to exclude from online posting.

As much as some senators may conclude that sharing all the movies you watch is TMI, the law should permit people to share as they choose, and companies should not face legal penalties for providing them with the choice.

*This article appeared on page A - 8 of the San Francisco Chronicle*



## Why They Track Us

By Jules Polonetsky and Christopher Wolf

 [May](http://www.huffingtonpost.com/technology/) 3, 2012

There has been much attention and debate over Web tracking for the past decade. Many of the concerns focus around behavioral advertising, the widespread practice of ad networks that use cookies to keep track of the site's users visit in order to tailor the ads they see across the Web. Advertising trade groups claim that the practice is needed to provide ads that are relevant to users. But critics consider the ads are subliminal, unfairly manipulating users based on secret information. Others are concerned about the creation of profiles that could be used to discriminate against users who visit health-related or other sensitive sites. And some just think the ads are creepy.

Industry has responded by labeling the ads with a symbol that is intended to alert users about the tracking and how they can opt-out of the targeting. The Federal Trade Commission has upped the ante, pressing for a Do Not Track feature that would allow users to tell websites via their browser that tracking was verboten. The Obama administration has jumped in, applauding a compromise agreement by trade groups to halt tailoring of ads when users activate the Do Not Track option.

The debate continues, with companies claiming the extra revenue from data-targeted ads is needed to support Web publishers and with advocates continuing to object to the practice as unfair.

The fireworks around behavioral ads have obscured many of the other, less provocative reasons that websites work with tracking companies. By setting a unique number, a cookie, on users' browsers, websites and advertisers can know how many unique users visited a website or saw an ad that was delivered across many sites. They can frequency cap an ad to make sure that each user sees the giant pop-up ad that slows access to the site only one time. By reading the same cookie relayed by a user on a website when an ad is delivered and then again when a user visits an advertiser's site, the company can learn which ads are bringing users to their site.

But what about users who see banner ads online and then end up purchasing at the store? Although online commerce is growing rapidly, most purchases are still made by users showing up in person at a store. Major offline retailers won't spend their dollars online without some understanding of whether the online ads they pay for are working. How can an advertiser who buys ads online learn that users who saw the ads are more likely to spend at their store than users who were not exposed to the ads?

Despite the challenge of the jump from virtual ad to physical store, savvy research analysts have long figured out how to provide advertisers with reports that do just that. Here is how it works: An advertiser buys ads that are delivered by an ad server on the site of a Web publisher such as AOL, Yahoo or the *Wall Street Journal* that has a substantial number of registered users. Each time an ad is delivered, a flag is added to the profile the publisher has about the user who saw the ad. The user's name is then hashed and the hash, with its flag, is sent to a service provider who will help join the "anonymized" data. That same service provider has been holding a similarly hashed copy of sales transactions from the retailer's customer database. The hashed users from the publisher are matched with the corresponding retailer data and a report is prepared. This summarized report tells the retailer, if the ads have been working, that customers who made large purchases or many purchases were more likely to have seen the advertiser's ads than the general audience.

This practice of tracking users to prepare summarized analytic reports such as this is now fairly commonplace. Some companies go to great lengths to ensure anonymity using encryption and third-party doubleblind processes via intermediaries to add privacy protections to the procedure. Leading companies are proud of their successful ad campaigns and publicize case studies proclaiming the prowess of their ads.

Some critics point out that TV, radio and magazine advertisers measure ad effectiveness using research panels of users who sign up to provide feedback. Why do websites need to measure effectiveness with greater precision, given the complaints about tracking? But these other media can rely on the power of their message which is supported by sound, pictures, and emotional stories. Users can recall the good ads, and the best become part of pop culture. "Good to the last drop" -- Maxwell House. "If I were an Oscar Meyer Weiner." "Mikey likes it!"

The tiny Web banner ad can hardly compete with TV, radio and magazines except for in one way, in being precisely measurable.

And that's the rest of the story.

*The authors are co-chairs of the Future of Privacy Forum, a think tank dedicated to advancing responsible data practices.*

******

**Privacy: Light Slap For Dharun Ravi; Big Penalties For Dot-Coms**

**

*June 1, 2012*

Internet technologies make the unwanted sharing of personal information possible. Nowhere was this more vividly demonstrated that in the recent case of Dharun Ravi, who rigged a webcam to spy on his gay roommate Tyler Clementi in a romantic encounter, and then gleefully Tweeted about it, leading to Clementi’s suicide. On March 16th, Ravi was found guilty by a New Jersey jury of 15 criminal charges including invasion of privacy, bias intimidation, tampering with evidence, and witness tampering. For those offenses, the judge sentences Ravi to 30 days in jail. Ravi could have been sentenced to a term on 10 years.

In a case where lawmakers have specified a range of penalties available to remedy privacy and related violations, it is fair to characterize Ravi’s punishment as a slap on the wrist. While the available punishment of 10 years seemed excessive since Ravi was not on trial for murder (even though Celementi’s death was linked to the episode), 30 days does not being to express society’s outrage at the multiple acts of criminal conduct found by the New Jersey jury – acts that showed reckless indifference to the privacy and dignity of another human being.

It may be tempting for some privacy advocates to draw a parallel between the lack of real relief for the privacy violations in the Ravi case and what they portray as the “free pass’” given companies that violate personal privacy by collecting and using personal information about people without their permission.

It is true in general that there are relatively few monetary remedies for invasions of privacy for plaintiffs who file lawsuits, although some privacy laws specifically provide for damages. But that does not mean that companies can get away with privacy violations. Unlike in the Ravi case, companies who violate consumer privacy face real enforcement and penalties few would consider “slaps on the wrist.”

The Federal Trade Commission is the most powerful “cop on the beat” when it comes to remedying privacy violations. Companies subject to FTC enforcement for deceptive and unfair practices face 20 year-long consent decrees with detailed requirements -essentially 20 years of reporting to a “privacy probation officer”. Facebook and Google were recent targets of the FTC and each is under a significant consent decree. The Department of Health and Human Services also has potent remedial powers under the health privacy law, HIPAA. Financial regulators enforce the financial privacy laws. Kids have special online privacy protections. And state Attorneys General increasingly are active under state consumer protection laws in going after companies deemed to violate personal privacy.

A series of privacy-violating acts in New Jersey leading to real harm – a person’s suicide – resulted in punishment more typical of convictions for excessive speeding violations. By contrast, privacy issues focused on by regulators frequently result in serious consequences for the investigated companies – 20 year consent decrees – even in cases where no specific consumer harm can be shown.

The privacy regulators often bring enforcement actions to teach corporate America a lesson, and to encourage better behavior. But the fact is that with thousands of companies employing Chief Privacy Officers, and with a new realization on the part of most businesses that privacy matters (as it creates needed consumer trust), companies for the most part have matured past an era of adolescent disregard for consumer privacy rights. Privacy is taken seriously in corporate America.

Empowered with tools (and toys) of technology, the same cannot necessarily be said about the Dharun Ravi generation. It is easy for teens to invade their peers’ privacy, and to cause real harm. One wonders whether the 30 day sentence Mr. Ravi received will teach any lessons or affect online behavior.

Had Ravi been an online company, he would be dealing with FTC enforcement staff for decades after his jail sentence is over.

Encryption and Globalization

[Peter](http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=69688) Swire, Ohio State University (OSU) - Michael E. Moritz College of Law and Kenesa Ahmad, Fellow, Future of Privacy Forum
Columbia Science and Technology Law Review (forthcoming 2012)
**Abstract:**
During the explosive growth of the Internet in the 1990s, encryption was quite likely the single most passionate area of legal and policy debate. Law enforcement and national security agencies supported limits on the export of strong encryption, fearing that encryption would block their ability to protect public safety and national security. Supporters of strong encryption most basically argued that encryption was essential to securing communication over the Internet. During the “crypto wars” of the 1990’s, government policy initially supported surveillance, with the Clipper Chip proposal and a policy of escrowing encryption keys. The administration shifted position in 1999, allowing export largely without restrictions. After this shift in policy, encryption law and policy largely faded from view.

Encryption is now resurfacing as a major issue, most visibly in India and China. Indian law currently forbids the use of encryption keys longer than 40 bits, which is far below international standards. China, meanwhile, insists that hardware and software made or used in China only employ cryptosystems developed in China.

The article seeks to fill an important gap in the literature. Because the U.S. encryption problem was “solved” in 1999, a new generation of policy makers, lawyers, and technologists has emerged with little or no experience in the area of encryption policy.

Part I of this article offers a short history of wiretaps for phone and Internet data, illustrating why communications across the Internet are far more vulnerable than traditional phone calls, unless encryption is used. Part II provides a primer on basic encryption concepts that are relevant to the subsequent legal and policy analysis.

Part III highlights key lessons learned from the U.S. crypto wars of the 1990s, informed by the perspective of one of the authors, who chaired the White House Working Group on Encryption in the lead-up to the 1999 change in U.S. encryption policy.

Part IV builds on the U.S. experience, and proposes two additional reasons why effective encryption becomes even more important when the debate shifts from one country to a globalized setting. The first is the large and growing importance of cybersecurity for nations around the world. In cybersecurity today, the “offense” (in the form of thousands of attacks per day) is significantly ahead of the “defense.” Cryptography is quite possibly the largest category of effective defensive tool. In a globalized world, security holes in major countries (such as India or China) directly lead to security holes elsewhere. Globalization also leads to what we call the “least trusted country problem -- the level of trust placed in data traveling through the Internet becomes that of the country that we trust least.

Part V synthesizes the key reasons supporting effective encryption in today’s globalized world, despite the security objections of law enforcement and national security agencies, and the trade interests of some countries. By examining the relevant history, technology, law, and policy, this article explains why it is vital to assure the widespread and global availability of strong encryption for our data and communications.

Swire, Peter P. and Ahmad, Kenesa, Encryption and Globalization (November 16, 2011). Ohio State Public Law Working Paper No. 157. Available at SSRN: http://ssrn.com/abstract=1960602 or http://dx.doi.org/10.2139/ssrn.1960602