What is privacy? 2

Privacy and Two Controversies 2

Area 1 -- Surveillance 6

Area 2 – Consumer Privacy 11

A Roadmap for Regulation 14

Status Quo Action – Surveillance Reform 14

-Many specific loopholes 14

-Even if legislation passes (a big if), it won’t reign in foreign intelligence surveillance will contain many loopholes 15

-Even if legislation passes as-is, it won’t contain a privacy advocate on the FIS court 16

-The bill may not end all authorities for metadata collection 16

-Surveillance could potentially expand if the cybersecurity bill passes 17

-Privacy groups have withdrawn support for the House version 18

Status Quo Action – Consumer Privacy 19

-No movement for consumer privacy protection now 19

Advantage Areas 19

Privacy and an Additional Controversy – Searches & the 4th Amendment (Area 3) 26

The Negative 28

Answering the Privacy Advantage 28

Disadvantages 30

Counterplans 33

Kritiks 34

Specific Plans – Surveillance 34

46 recommendations 34

Repeal or modify Executive Order 12333 40

Repeal or modify section 702 42

FISA court reform – special advocate 44

General improvements and transparency 44

Amendments to USA Freedom Act 45

Additional proposed reforms 46

Additional (2) proposed reforms 46

Extend privacy rights to EU citizens 47

Specific Plans—Consumer Privacy Protection 48

4 plans 48

Testimony related to protecting consumer financial privacy 49

Specific Plans – 4th Amendment 50

Wording a Resolution 50

Benefits to Debating the Topic 52

Concerns with Debating the Topic 52

Additional General Background on Privacy 52

Bibliopgrahy – NSA Surveillance (web resources) 53

Bibliography – Law Reviews on Privacy 74

## What is privacy?

“Privacy” is a broad idea that includes many ideas such as freedom of thought, control over one’s body, solitude in one’s home, control over information about oneself, freedom from surveillance, protection of one’s reputation, and protection from searches and interrogation.

Daniel Solove, Assistant Professor of Law, Seton Hall Law School. J.D., Yale Law School, 2002, California Law Review, “Conceptualizing Privacy,” p. 1088-9

Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, *control over information about oneself, freedom from surveillance*, protection of one's reputation, and protection from searches and interrogations. Time and again philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy.  Arthur Miller has declared that privacy is "difficult to define because it is exasperatingly vague and evanescent."  According to Julie Inness, the legal and philosophical discourse of privacy is in a state of "chaos." Alan Westin has stated that "few values so fundamental to society as privacy have been left so undefined in social theory ... ." William Beaney has noted that "even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right."  Privacy has "a protean capacity to be all things to all lawyers," Tom Gerety has observed. According to Robert Post, "privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all." Several theorists have surveyed the interests that the law protects under the rubric of privacy and have concluded that they are distinct and unrelated. Judith Thompson has even argued that privacy as a concept serves no useful function, for what we call privacy really amounts to a set of other more primary interests.

Although some of these areas overlap (e.g., controlling information about oneself can protect one’s reputation), this topic proposal is focused on policy proposal that protect control over information about oneself and freedom from surveillance. It is possible to consider broadening the topic to include searches and interrogations, and that is discussed briefly at the end of the paper, but that it is not the focus.

## Privacy and Two Controversies

The controversy related to control of one’s information and protection against surveillance is related to basic issues/disputes. The first concerns protection of information that online media companies such as Google and Facebook have on us. For example, yesterday I noted that Google knew what hotel I was staying in and where I was having dinner even though I didn’t register for the hotel or dinner through Google, or even find either place through a Google search. It likely knew what hotel I was staying in through online tracking and where I was having dinner because Opentable.com shared information with it.

In a recent (May 2014) Report to the President – [Big Data and Privacy: A Technological Perspective](mailto:http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf) – The President’s Council of Advisors on Science & Technology wrote:

The ubiquity of computing and electronic communication technologies has led to the exponential growth of data from both digital and analog sources. New capabilities to gather, analyze, disseminate, and preserve vast quantities of data raise new concerns about the nature of privacy and the means by which individual privacy might be compromised or protected. After providing an overview of this report and its origins, Chapter 1 describes the changing nature of privacy as computing technology has advanced and big data has come to the fore. The term privacy encompasses not only the famous “right to be left alone,” or keeping one’s personal matters and relationships secret, but also the ability to share information selectively but not publicly. Anonymity overlaps with privacy, but the two are not identical. Likewise, the ability to make intimate personal decisions without government interference is considered to be a privacy right, as is protection from discrimination on the basis of certain personal characteristics (such as race, gender, or genome). Privacy is not just about secrets. Conflicts between privacy and new technology have occurred throughout American history. Concern with the rise of mass media such as newspapers in the 19th century led to legal protections against the harms or adverse consequences of “intrusion upon seclusion,” public disclosure of private facts, and unauthorized use of name or likeness in commerce. Wire and radio communications led to 20th century laws against wiretapping and the interception of private communications – laws that, PCAST notes, have not always kept pace with the technological realities of today’s digital communications.

Past conflicts between privacy and new technology have generally related to what is now termed “small data,” the collection and use of data sets by private‐ and public‐sector organizations where the data are disseminated in their original form or analyzed by conventional statistical methods. Today’s concerns about big data reflect both the substantial increases in the amount of data being collected and associated changes, both actual and potential, in how they are used.

Big data is big in two different senses. It is big in the quantity and variety of data that are available to be processed. And, it is big in the scale of analysis (termed “analytics”) that can be applied to those data, ultimately to make inferences and draw conclusions. By data mining and other kinds of analytics, nonobvious and sometimes private information can be derived from data that, at the time of their collection, seemed to raise no, or only manageable, privacy issues. Such new information, used appropriately, may often bring benefits to individuals and society – Chapter 2 of this report gives many such examples, and additional examples are scattered throughout the rest of the text. Even in principle, however, one can never know what information may later be extracted from any particular collection of big data, both because that information may result only from the combination of seemingly unrelated data sets, and because the algorithm for revealing the new information may not even have been invented at the time of collection.

The same data and analytics that provide benefits to individuals and society if used appropriately can also create potential harms – threats to individual privacy according to privacy norms both widely shared and personal. For example, large‐scale analysis of research on disease, together with health data from electronic medical records and genomic information, might lead to better and timelier treatment for individuals but also to inappropriate disqualification for insurance or jobs. GPS tracking of individual might lead to better community‐based public transportation facilities, but also to inappropriate use of the whereabouts of individuals. A list of the kinds of adverse consequences or harms from which individuals should be protected is proposed in Section 1.4. PCAST believes strongly that the positive benefits of big‐data technology are (or can be) greater than any new harms.

Chapter 3 of the report describes the many new ways in which personal data are acquired, both from original sources, and through subsequent processing. Today, although they may not be aware of it, individuals constantly emit into the environment information whose use or misuse may be a source of privacy concerns. Physically, these information emanations are of two types, which can be called “born digital” and “born analog.”

When information is “born digital,” it is created, by us or by a computer surrogate, specifically for use by a computer or data processing system. When data are born digital, privacy concerns can arise from over‐collection. Over‐collection occurs when a program’s design intentionally, and sometimes clandestinely, collects information unrelated to its stated purpose. Over‐collection can, in principle, be recognized at the time of collection. When information is “born analog,” it arises from the characteristics of the physical world. Such information becomes accessible electronically when it impinges on a sensor such as a camera, microphone, or other engineered device. When data are born analog, they are likely to contain more information than the minimum necessary for their immediate purpose, and for valid reasons. One reason is for robustness of the desired “signal” in the presence of variable “noise.” Another is technological convergence, the increasing use of standardized components (e.g., cell‐phone cameras) in new products (e.g., home alarm systems capable of responding to gesture). Data fusion occurs when data from different sources are brought into contact and new facts emerge (see Section 3.2.2). Individually, each data source may have a specific, limited purpose. Their

combination, however, may uncover new meanings. In particular, data fusion can result in the identification of individual people, the creation of profiles of an individual, and the tracking of an individual’s activities. More broadly, data analytics discovers patterns and correlations in large corpuses of data, using increasingly powerful statistical algorithms. If those data include personal data, the inferences flowing from data analytics may then be mapped back to inferences, both certain and uncertain, about individuals. Because of data fusion, privacy concerns may not necessarily be recognizable in born‐digital data when they are collected. Because of signal‐processing robustness and standardization, the same is true of born‐analog data – even data from a single source (e.g., a single security camera). Born‐digital and born‐analog data can both be combined with data fusion, and new kinds of data can be generated from data analytics. The beneficial uses of near‐ubiquitous data collection are large, and they fuel an increasingly important set of economic activities. Taken together, these considerations suggest that a policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth). If collection cannot, in most cases, be limited practically, then what? Chapter 4 discusses in detail a number of technologies that have been used in the past for privacy protection, and others that may, to a greater or lesser extent, serve as technology building blocks for future policies. Some technology building blocks (for example, cybersecurity standards, technologies related to encryption, and formal systems of auditable access control) are already being utilized and need to be

encouraged in the marketplace. On the other hand, some techniques for privacy protection that have seemed encouraging in the past are useful as supplementary ways to reduce privacy risk, but do not now seem sufficiently robust to be a dependable basis for privacy protection where big data is concerned. For a variety of reasons, PCAST judges anonymization, data deletion, and distinguishing data from metadata (defined below) to be in this category. The framework of notice and consent is also becoming unworkable as a useful foundation for policy. Anonymization is increasingly easily defeated by the very techniques that are being developed for many legitimate applications of big data. In general, as the size and diversity of available data grows, the likelihood of being able to re‐identify individuals (that is, re‐associate their records with their names) grows substantially. While anonymization may remain somewhat useful as an added safeguard in some situations, approaches that deem it, by itself, a sufficient safeguard need updating. While it is good business practice that data of all kinds should be deleted when they are no longer of value, economic or social value often can be obtained from applying big data techniques to masses of data that were otherwise considered to be worthless. Similarly, archival data may also be important to future historians, or for later longitudinal analysis by academic researchers and others. As described above, many sources of data contain latent information about individuals, information that can be known only if the holder expends analytic resources, or that may become knowable only in the future with the development of new data‐mining algorithms. In such cases it is practically impossible for the data holder even to surface “all the data about an individual,” much less delete it on any specified schedule or in response to an individual’s request. Today, given the distributed and redundant nature of data storage, it is not even clear that data, even small data, can be destroyed with any high degree of

assurance. As data sets become more complex, so do the attached metadata. Metadata are ancillary data that describe properties of the data such as the time the data were created, the device on which they were created, or the destination of a message. Included in the data or metadata may be identifying information of many kinds. It cannot today generally be asserted that metadata raise fewer privacy concerns than data. Notice and consent is the practice of requiring individuals to give positive consent to the personal data

collection practices of each individual app, program, or web service. Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent.

Wired Magazine wrote nearly a year ago:

**Wired, 10-11**, 13, <http://www.wired.com/business/2013/10/private-tracking-arms-race/>

Thanks to former NSA man Edward Snowden, we now know [a fair amount](http://www.theguardian.com/world/the-nsa-files) about the NSA’s ability to collect data about what people do online, and it’s all rather disturbing.¶ But **the future looks even more worrisome. Some of the biggest companies in tech are assembling new forms of online tracking that would follow users more aggressively than the open technologies used today**. **Just this week, word arrived that Microsoft is developing such a system, following, apparently, in the footsteps of Google.¶ The new data troves are to be used for advertising, not government surveillan**ce, and only made available to authorized third parties. Yet the NSA has proven adept at co-opting large pools of data for its own ends.¶ “Users did not have much control in the cookie era,” says Marc Rotenberg, executive director of the Electronic Privacy Information Center, a nonprofit advocacy group in Washington. “But the problem is about to get much worse — **tracking techniques will become more deeply embedded and a much smaller number of companies will control advertising data.”¶** Rotenberg says potential NSA use of the next-generation tracking data is all the more reason to move away from behavioral tracking. And he points out that there’s already evidence that ad data could have been used by government spies. NSA documents [published](http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document) by the Guardian earlier this month [appear to postulate](http://arstechnica.com/security/2013/10/how-the-nsa-might-use-hotmail-or-yahoo-cookies-to-identify-tor-users/) that cookies set by the pervasive Google-owned ad network DoubleClick could be used to spot internet users who also use the Tor anonymity system.¶ The NSA Tor attack could only work on people who made mistakes using what is otherwise a strong system. But yesterday, [**Ad Age**](http://adage.com/article/digital/microsoft-cookie-replacement-span-desktop-mobile-xbox/244638/) **reported that Microsoft is developing a system that has intimate tracking at its core, following people as they hop from the web to apps and from PCs to tablets to phones to videogame consoles. By shoving aside cookies for an unspecified new identification technology built into devices at a lower level, Microsoft and its authorized partners would gain detailed tracking ability** — though the report also says that the system could lock out non-authorized parties, who are harder to exclude from the data flow in cookie-based tracking.¶ That may sound like a good thing, but keep in mind that Snowden’s documents indicate that the NSA has previously helped itself to big company data, with authorization or without.¶ Under Microsoft’s system, web “search data could inform TV-style ads within streaming video apps on Xbox,” Ad Age wrote. “Microsoft’s cookie replacement would essentially be a device identifier, meaning consumers could give permission for its advertising use when opting in to a device’s regular user agreement or terms of service.” Requiring an opt-in is better than not, but the reality is that most people opt in to such things, simply because services require or encourage them to do so.¶ Asked about the reported tracking system, a Microsoft spokesperson passed along the following written statement: “Microsoft believes going beyond the cookie is important. Our priority will be to find ways to do this that respect the interests of consumers. We have nothing further to share.” It’s not clear whether Microsoft’s system could be curbed by systems like the Tor Browser, which is designed to thwart older tracking strategies based on open standards.¶ Google is [reportedly](http://www.usatoday.com/story/tech/2013/09/17/google-cookies-advertising/2823183/) developing a similar cookie replacement scheme known as AdId. Indeed, large internet companies appear to be locked in [something of a tracking arms race](http://www.wired.com/business/2013/05/marissa-mayer-makes-portals-fashionable/) in an effort to sell increasingly targeted ads. **Facebook, for example, has added advertisements based on searches and web surfing conducted outside of Facebook and even based on what groceries you buy.** Still, it has relied on old, longstanding tracking techniques for which many blocking options exist. Microsoft and Google are contemplating closely held systems that could be much harder to fight.¶ Right now, ordinary internet users are more angry than they’ve ever been about the government sweeping their private data into big, concentrated surveillance databases. At the same time**, large corporations are eagerly improving their ability to sweep private data into big, concentrated advertising databases.**

### Area 1 -- Surveillance

The controversy between national security objectives and privacy became a hot one for debate since it was [disclosed in June of 2013](http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order) by former defense contractor (supported by journalist [Glenn Greenwald](http://en.wikipedia.org/wiki/Glenn_Greenwald)) [Edward Snowden](http://en.wikipedia.org/wiki/Edward_Snowden) that the NSA is engaging in extensive surveillance inside the United States in order to fight crime and reduce the threat of terrorism.  The magnitude of the disclosure shocked many people, including elected representatives, who were unaware of the extent of the surveillance.  Many civil rights advocates view the surveillance as an assault on liberty while law enforcement and national security officials see the programs as essential weapons in the war on terror, the fight against nuclear weapons proliferation, and the general protection of US national security.

Stuart **Taylor, April 29, 2014,** The Big Snoop: Life, Liberty, and the Pursuit of Terrorists,  <http://www.brookings.edu/research/essays/2014/the-big-snoop-print> (is an author, a freelance journalist, and a Brookings nonresident senior fellow. Taylor has covered the Supreme Court for a variety of national publications, including The New York Times, Newsweek, and National Journal, where he is also a contributing editor. His published books include Mismatch: How Affirmative Action Hurts Students It's Intended to Help, and Why Universities Won't Admit It. In addition to his work as a journalist and scholar, he is a graduate of Harvard Law School and practiced law in a D.C. firm.)

In the months before 9/11, Joel Brenner had been trying cases as a founding partner in a Washington, D.C. law firm. As he walked home from work that Tuesday evening, fires were still burning at the Pentagon. It was then that he decided he wanted to go to work for “the people who were chasing the bastards who were blowing us up.” He spent four years as the NSA’s inspector general, then three years as the nation’s top counterintelligence official, and then another 15 months as the NSA’s senior counsel.

**Ron Wyden** also joined the nearly unanimous vote for the Patriot Act shortly after the 9/11 attacks. But before long he came to a conclusion that was nearly the opposite of Feinstein’s and Brenner’s. He worried that the pendulum was swinging too far away from a proper regard for the Constitution and would inevitably lead to abuses by the intelligence community. **In 2003,** he **led the battle in the Senate that defunded the Total Information Awareness program, a Pentagon unit established to hunt down terrorists by scouring mountains of data to reconstruct the electronic footprints of millions of people.**

However, just as Wyden feared, the prevailing sentiment on Capitol Hill was that the reforms of the 1970s had impeded the NSA from uncovering the 9/11 plot in time to prevent the attacks. It was in that atmosphere that two new programs were put into place during George W. Bush’s presidency.

**In 2006, the FISA Court secretly authorized the NSA to collect from phone companies the records of trillions of phone calls made within, to, or from the United States for analysis and storage.** The purpose of this gigantic undertaking was to identify foreign terrorists’ actual, possible, or potential collaborators who were on American soil. **It came to be known as the “bulk phone records program,” or the “Section 215 program,”** after a provision in the Patriot Act that allowed the government to demand access to “any tangible things,” so long as the government specified that they were “relevant to an authorized investigation… to protect against international terrorism or clandestine intelligence activities.”

Two years later, **near the end of the Bush presidency, Congress passed Section 702,** an amendment to the Foreign Intelligence Surveillance Act, authorizing the targeting of communications of “foreign persons who are located abroad.” **This provision became the basis for sweeping, clandestine NSA programs including one called PRISM, an acronym for “Planning Tool for Resource Integration, Synchronization, and Management.” It was actually a gargantuan collection tool that enabled the NSA to gather from U.S.-based Internet companies hundreds of millions of emails, Internet voice calls, videos, photos, chat services, stored data, and other private Internet communications,** if the targets were “reasonably believed” to be non-U.S. persons overseas who possessed “foreign intelligence information.”

Unlike the phone-records program, PRISM made available to the NSA the contents of the communications that were collected. At least nine U.S.-based companies were compelled by the surveillance court to cooperate with the NSA in facilitating access to PRISM data: Google, Facebook, Microsoft, Apple, Yahoo!, Paltalk, AOL, YouTube, and Skype. The companies rarely appealed court orders, and complied with alacrity. Patriotism was certainly a factor, but so was their reliance on the government for business, security clearances, help with network security, and other benefits.

At the same time that public trust in the government was in something close to free fall, **the digital revolution was gathering momentum, and the NSA was taking full advantage of it**. **Moore’s Law had made possible an exponential leap in the capacity to gather, store, and sift through trillions of electronic communications, both internationally and within the United States. That gave the intelligence agencies potentially invaluable tools for tracking spies, criminals,**and—ever since 9/11—the new Public Enemy No. 1: terrorists. With terrorists using cell phones, the Internet, and commercially available encryption software to conceal themselves, communicate covertly, and plan acts of mass murder, officials charged with defending the United States were all the more determined to make the most of the new means of gathering and analyzing information.

The result was a particularly dramatic manifestation of the tendency for a transformative technology to outpace its own regulation. Before the Snowden leaks, the two most significant examples of this phenomenon were the invention of the steam engine, which made possible the Industrial Revolution but also triggered the process of climate change, and the harnessing of the power of the atom, which could help light up the world with clean energy but could also incinerate it in global thermonuclear war. **The Snowden leaks brought to light a third example: a revolution that has made it possible for us to communicate more easily, but also for our government to collect and analyze our communications on a scale that the phrase “Big Data” does not begin to capture. This exponential leap in the ability to collect and crunch data has—to a dizzying degree and at a dizzying pace—run roughshod over laws, standards of conduct, and international norms, leading many observers to conclude that the law as currently written is inadequate to maintain the balance between national security and individual privacy called for by the Fourth Amendment.**

A recent (July 5th) Washington Post [article details that Americans who are not the target of the surveillance are more likely to be subjected to surveillance than the targets themselves.](http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?hpid=z1)

[Peter Van Buren](http://www.tomdispatch.com/post/175861/tomgram%3A_peter_van_buren,_what_we%27ve_lost_since_9_11_%28part_2%29/) explained how widespread and pervasive government surveillance is and can be on June 25, 2014

More of life is now online -- from banking to travel to social media. Where the NSA was once limited to traditional notions of communication -- the written and spoken word -- new possibilities for following you and intruding on your life in myriad ways are being created. The agency can, for instance, now collect images, photos, and video, and subject them to facial recognition technology that can increasingly put a name to a face. Such technology, employed today at casinos as well as in the secret world of the national security state, can pick out a face in a crowd and identify it, taking into account age, changes in facial hair, new glasses, hats, and the like.

An offshoot of facial recognition is the broader category of biometrics, the use of physical and biological traits unique to a person for identification. These can be anything from ordinary fingerprinting to cutting-edge DNA records and iris scans. (Biometrics is already big business and even has its own trade association in Washington.) One of the world's largest known collections of biometric data is held by the Department of State. As of December 2009, its Consular Consolidated Database (CCD) contained more than 75 million photographs of Americans and foreigners and is growing at a rate of approximately 35,000 records per day. CCD also collects and stores indefinitely the fingerprints of all foreigners issued visas.

With ever more data available, the NSA and other agencies are creating ever more robust ways to store it. Such storage is cheap and bounteous, with few limits other than the availability of electricity and water to cool the electronics. Emerging tech will surely bypass many of the existing constraints to make holding more data longer even easier and cheaper. The old days of file cabinets, or later, clunky disk drives, are over in an era of mega-data storage warehouses.

The way data is aggregated is also changing fast. Where data was once kept in cabinets in separate offices, later in bureaucratically isolated, agency-by-agency digital islands, post-9/11 sharing mandates coupled with new technology have led to fusion databases. In these, information from such disparate sources as license plate readers, wiretaps, and records of library book choices can be aggregated and easily shared. Basically everything about a person, gathered worldwide by various agencies and means, can now be put into a single 'file.'

Once you have the whole haystack, there's still the problem of how to locate the needle. For this, emerging technologies grow ever more capable of analyzing Big Data. Some simple ones are even available to the public, like IBM's Non-Obvious Relationship Awareness software (NORA). It can, for example, scan multiple databases, geolocation information, and social media friend lists and recognize relationships that may not be obvious at first glance. The software is fast and requires no human intervention. It runs 24/7/365/Forever.

Tools like NORA and its more sophisticated classified cousins are NSA's solution to one of the last hurdles to knowing nearly everything: the need for human analysts to 'connect the dots.' Skilled analysts take time to train, are prone to human error, and -- given the quickly expanding supply of data -- will always be in demand. Automated analysis also offers the NSA other advantages. Software doesn't have a conscience and it can't blow the whistle.

Although conducted by different entities (private companies and the government) and for different reasons (commercial gain and security) both actions invade a person’s privacy, defined (in this instance) as the ability to protect information about themselves that collected online. In most instances these controversies overlap, because the US National Security Agency (NSA) works with private companies to collect information on individual users. Additional information about NSA programs is detailed in the next section.

[According to Wikipedia](http://en.wikipedia.org/wiki/National_Security_Agency), “the National Security Agency (NSA) is the main producer and manager of [signals intelligence](http://en.wikipedia.org/wiki/Signals_intelligence) for the [United States](http://en.wikipedia.org/wiki/United_States). Estimated to be one of the largest of [U.S. intelligence organizations](http://en.wikipedia.org/wiki/US_intelligence_community#Organization) in terms of personnel and budget, the NSA operates under the jurisdiction of the [Department of Defense](http://en.wikipedia.org/wiki/United_States_Department_of_Defense) and reports to the [Director of National Intelligence](http://en.wikipedia.org/wiki/Director_of_National_Intelligence). The NSA is primarily tasked with global monitoring, collection, [decoding](http://en.wikipedia.org/wiki/Codebreaking), translation and analysis of information and data for foreign intelligence and [counterintelligence](http://en.wikipedia.org/wiki/Counterintelligence) purposes, including surveillance of targeted individuals on U.S. soil. The agency is authorized to accomplish its mission through [clandestine means](http://en.wikipedia.org/wiki/Clandestine_operations), among which is [bugging](http://en.wikipedia.org/wiki/Bugging) electronic systems[9] and allegedly engaging in [sabotage](http://en.wikipedia.org/wiki/Sabotage) through [subversive software](http://en.wikipedia.org/wiki/Stuxnet). The NSA is also responsible for the [protection](http://en.wikipedia.org/wiki/Information_security) of [U.S. government](http://en.wikipedia.org/wiki/Federal_Government_of_the_United_States) communications and [information systems](http://en.wikipedia.org/wiki/Information_systems).” It has a 10.8 billion dollar budget.

Domestic mass surveillance  (though it is usually directed at foreign sources (a larger discussion of this follows below)) is conducted by the NSA through a number of programs. There is no official, comprehensive list of NSA programs.  Most of the programs are “classified,” meaning that they are not public, and the only reason that we even know about many of them is because of the disclosures of [Edward Snowden](http://en.wikipedia.org/wiki/Edward_Snowden). Since we rely on disclosures to learn about the programs, and since all of the disclosing is relatively recent, it is the case that new programs are continually disclosed. In fact, it is likely that between now (May 3) and when you finish debating the topic (mid-June) that [more programs will be disclosed](http://www.miamiherald.com/2013/10/03/3666598/nsa-reveals-more-about-its-spying.html).

*Metadata collection.* One of the most publicized and debated programs is NSA’s metadata program that collects information on phone calls from hundreds of millions of cell phone and Skype subscribers as well as from popular email services such as Gmail and Yahoo.  In June,2013, the Guardian disclosed that the Foreign Intelligence Surveillance Court (FISC) issues a classified order that required Verizon should pass the government “an electronic copy of metadata ‘created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.’”

[Social networking data is also included](http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html).  According to the New York Times explains:

Since 2010, the [National Security Agency](http://topics.nytimes.com/top/reference/timestopics/organizations/n/national_security_agency/index.html?inline=nyt-org) has been exploiting its huge collections of data to create sophisticated graphs of some Americans’ social connections that can identify their associates, their locations at certain times, their traveling companions and other personal information, according to newly disclosed documents and interviews with officials…. The policy shift was intended to help the agency “discover and track” connections between intelligence targets overseas and people in the United States, according to an N.S.A. memorandum from January 2011. The agency was authorized to conduct “large-scale graph analysis on very large sets of communications metadata without having to check foreignness” of every e-mail address, phone number or other identifier, the document said…. The agency can augment the communications data with material from public, commercial and other sources, including bank codes, insurance information, Facebook profiles, passenger manifests, voter registration rolls and GPS location information, as well as property records and unspecified tax data, according to the documents. They do not indicate any restrictions on the use of such “enrichment” data, and several former senior Obama administration officials said the agency drew on it for both Americans and foreigners.

The [Guardian reported](http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents) on September 30, 2013 that this metadata collection includes “browsing history – such as map searches and websites visited – to account details, email activity, and even some account passwords” and that it is retained for an entire year in a storage system called Marina.  Phone meta data is stored in a different system.

Email address books and chats.  On October 14, 2013, the Washington Post revealed that the NSA was collecting [hundreds of millions of email address books and chat logs](http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html).

NSA Chief General Keith Alexander [denies monitoring social networks](http://www.miamiherald.com/2013/10/03/3666598/nsa-reveals-more-about-its-spying.html) of Americans, but said that data could be swept up if those Americans are connected to those suspects through phone calls or other data.

The Guardian original broke the NSA metadata story when it released documents obtained by Snowden that showed that Verizon was required to turn over phone meta data for all of its customers .  Follow-up reporting by the Washington Post showed that this program has been going on for years, with the government collecting metadata Sprint Nextel, AT&T and Bell South since 2006.  Billions of phone records are stored in a database called MAINWAY.

This data collection is referred to as “metadata” because the NSA claims that it does not actually monitor the *contents* of the communications but only the number of communications, the frequency of the communications, and the numbers/email addresses being communicated with. This information is stored (it is believed to be stored for 5 years) and, if necessary (if illegal activity is suspected) then a warrant could be obtained for the contents.

There is some debate as to whether or not the contents of the communication is collected. Although some proponents of the metadata program claim that the content is not monitored, others claim that the content of the emails is collected through a program called xKeyscore but that the emails are not read unless there is “a nexus to al-Qaida or other terrorist groups.”

The data that the NSA provides to the FBI is just the phone number, the date, and the time and duration of the call. It does not include the names of either of the callers.   Even then, this data can only be accessed during an investigation. If the number of a terrorist is connected to an American, the FBI needs a court order to take any action against the American.

According to Congressional testimony on October 2, 2013, this program began as part of a “pilot project” (a test program) to determine if the NSA could effectively keep track of user’s location by [monitoring their connections to various cell phone towers](http://www.slate.com/blogs/future_tense/2013/10/02/keith_alexander_admits_the_nsa_tracked_americans_cellphones_in_pilot_project.html?wpisrc=burger_bar)., potentially [even when their phones are turned off](http://www.slate.com/blogs/future_tense/2013/07/22/nsa_can_reportedly_track_cellphones_even_when_they_re_turned_off.html). An August 9,  2013 Guardian report [explains the details of the program](http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls).

This metadata that is collected from web service providers (Google, Microsoft, Facebook, etc) is collected through program called PRISM. There were initial media reports that portrayed PRISM as an automatic suction pipe that was connected to Google, Microsoft and Facebook servers (among others) that would automatically suck out data from those servers and deposit that data on NSA servers. Although PRISM does exist, these initial media reports are considered to be inaccurate. PRISM does collect data from these companies, but it only connects and collects data that is approved by FISC. It is not an automatic back door pipe.

The NSA is required to "minimize" the data of US persons, but is permitted to keep US communications where it is not technically possible to remove them, and also to keep and use any "inadvertently" obtained US communications if they contain intelligence material, evidence of a crime, or if they are encrypted.”

The NSA justifies this metadata collection program based on an interpretation of S[ection 215](https://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-section-215) of [the PATRIOT Act](http://en.wikipedia.org/wiki/Patriot_Act) whereby the entirety of US communications records may be considered "relevant" to a terrorism investigation if there is reasonable belief that even a tiny minority of the communications in this data-set may relate to terrorism.  Section 215 permits the government to collect “business records” that are relevant to a terrorism investigation and the government argues that the metadata that is collected by these companies is  a business record.  The PATRIOT Act was passed after the 2001 terrorist attacks and radically expanded government surveillance and policing authority.

Although NSA officials deny the metadata collection today continues under the PATRIOT Act, others suggest that perhaps it still continues under the [Foreign Intelligence Surveillance Act (FISA](http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act)), which was passed in 1978 to limit previous abuses by the government. [Section 702 of FISA “allows for the collection of data without individual warrants of communicatio](http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents)ns, where at least one end of the conversation, or data exchange, involves a non-American located outside the US at the time of collection. This section, which allows the collection of communications from Americans when they are “incidental” to foreign intelligence gathering was added as an amendment to FISA in 2008.  The NSA can store this data for up to 5 years if  the material is deemed relevant to “foreign intelligence” or if it is suspected of having “secret meaning”

There is a Foreign Intelligence Surveillance Court (FISC) that is charged with overseeing these programs in order to minimize/prevent rights violations, but the court is not an investigative one and cannot investigate non-compliance with the NSA’s own rules.  Since many members of Congress were not even aware of the existence of these programs, their own oversight is obviously limited.

Individuals who constructed the program, along Department of Defense and Department of Justice lawyers, believe it is legal based on a 1979 Supreme Court cases that said that individuals had no expectation of privacy in the numbers that they called, only in the content of the conversations. Given this, meta data collection itself is not subject to review by the Foreign Intelligence Surveillance Court.

*Encryption cracking****.*** The NSA has put pressure on private companies to weaken their own encryption of private data to make larger amounts of data more vulnerable to surveillance by the NSA. Recent stories indicate that the NSA is also aggressively expanding its [encryption breaking programs](http://www.businessinsider.com/nsa-snowden-hackers-2013-10).

For more on NSA surveillance and the history of the programs, see [Timeline of NSA Domestic Spying](https://www.eff.org/nsa-spying/timeline), [NSA Warrantless Surveillance (2001-2007](http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_%282001%E2%80%9307%29)).

### Area 2 – Consumer Privacy

[USA Today](mailto:http://www.usatoday.com/story/tech/2014/07/03/facebook-emotion-study-complaint-epic/12157471/%20), July 3

SAN FRANCISCO — A privacy watchdog group filed a [formal complaint](http://epic.org/privacy/ftc/facebook/Facebook-Study-Complaint.pdf) with the Federal Trade Commission claiming Facebook broke the law when it conducted a study on the emotions of its users without their knowledge or consent.

The Electronic Privacy Information Center filed the complaint on Thursday.

The complaint alleges Facebook deceived users by secretly conducting a psychological experiment to explore if seeing positive or negative updates in their news feeds would sway their emotions.

"At the time of the experiment, Facebook did not state in the Data Use Policy that user data would be used for research purposes. Facebook also failed to inform users that their personal information would be shared with researchers," the complaint says.

Facebook issued a statement in response to the complaint.

"When someone signs up for Facebook, we've always asked permission to use their information to provide and enhance the services we offer. To suggest we conducted any corporate research without permission is complete fiction," the statement says. "Companies that want to improve their services use the information their customers provide, whether their privacy policy uses the word 'research' or not."

Jeffrey Chester, executive director of the Center for Digital Democracy, said he has also reached out to regulators and is considering filing his own complaint.

"We are speaking to the FTC next week about the potential violation," Chester said.

Facebook is already facing an investigation from British regulators.

Facebook is under a settlement agreement with the FTC over privacy issues, but the settlement was reached in August 2012 after the one-week study was conducted.

Facebook Chief Operating Officer Sheryl Sandberg apologized on Wednesday, saying the study was part of "ongoing research" to test products and was "poorly communicated."

The experiment has angered Facebook users who have protested on Facebook and social media.

The complaint from the Electronic Privacy Information Center echoed those protests.

"The company purposefully messed with people's minds," it says.

[Consumer Reports](mailto:http://www.clarksvilleonline.com/2014/06/21/consumer-reports-survey-shows-62-percent-online-consumers-nothing-protect-internet-privacy/), June 21

Despite a rash of high-profile data breaches and cyber threats, an alarming 62 percent of U.S. online consumers have done nothing to protect their privacy on the Internet, according to a recent national Consumer Reports survey.

Perhaps not surprisingly, the number of victims is on the rise. One in seven online consumers were notified that their personal data had been breached in 2013 – a 56 percent increase from 2012. And a projected 11.2 million people fell for e-mail phishing scams, up 22 percent from the previous year.

[Privacy & Security Law Blog](mailto:http://www.jdsupra.com/legalnews/ftc-releases-2014-privacy-and-data-secur-10560/), July 4,

Last week, the Federal Trade Commission (FTC) released its [*2014 Privacy and Data Security Update*](http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf), summarizing the FTC’s major enforcement actions, policy initiatives, rules, reports, workshops, and outreach efforts in the privacy and data security arenas from approximately January 2013 until March 2014. In the 2014 Update, the FTC underscores its commitment to educating consumers, businesses and other stakeholders through its publications and roundtables on how to guard consumer privacy expectations and comply with applicable federal laws. Education, however, is accompanied by enforcement, and the FTC includes a long-list of recent actions against individuals and enterprises, which demonstrates that the FTC is not shy about using its broad regulatory authority to protect consumer privacy. Of major note were the FTC’s actions against companies for unfair or deceptive trade practices; its settlements with U.S. businesses for falsely asserting compliance with the U.S.-E.U. Safe Harbor Framework; the FTC’s updates to the COPPA regulatory rule; and its continued efforts to take telemarketers to task for violating the Do-Not-Call provisions of the Telemarketing Sales Rule.

[Health Security](mailto:http://healthitsecurity.com/2014/07/18/do-third-parties-regularly-access-consumer-health-data/), July 18

Consumer-generated healthcare data privacy doesn’t appear to have caused too many ripples in the general public’s consciousness to this point. But a recent [California Healthcare Foundation report](http://www.chcf.org/publications/2014/07/heres-looking-personal-health-info" \t "_blank) looks at how personal health information is tracked and used.

From using Google to search for health-related information to using mobile applications to track and monitor eating or exercise activity, consumers consistently leave their digital health marks without knowing they’re doing so. And this trend is growing in popularity, as the report said that wearable fitness device purchases had tripled from 3 percent in 2012 to 9 percent in 2013. There are tremendous opportunities for [data mining](http://healthitsecurity.com/glossary/data-mining/), but there are certainly still loose ends from a privacy perspective.

Because this consumer health information often doesn’t go through HIPAA covered entities, this space is a “wild west” of sorts in that consumers can’t be sure their data has been de-identified.

While personal health information held by healthcare providers and insurers is protected under HIPAA, many other sources of consumer data are not covered and can be disclosed to third parties. Unless and until a patient shares user-generated data with a HIPAA covered entity, the information is not covered by HIPAA. User-generated data that could be used in health profiling are held by gyms, websites, banks credit card companies . . .

[Cameron Kerry,](mailto:http://www.brookings.edu/blogs/techtank/posts/2014/07/1-kerry-microsoft-future-privacy) July 1

The truth is that there is a lot to be gained by third parties when it comes to patient data and having a better understanding of their trends and habits, even if the data isn’t technically health information. For example, Deven McGraw, partner at Manatt, Phelps and Phillips, said that while the FICO Medical Adherence Score isn’t based on health data, but instead demographic information that gives great insight into medication adherence. “Digital dust can have health implications even if the ‘dust’ is devoid of actual health information,” she said.

Regulating the privacy of information deemed to be health information and mere demographic data created by consumer mobile health applications or web browsing is undoubtedly an interesting topic. Even the [Apple HealthKit app as part of iOS 8](http://healthitsecurity.com/2014/06/11/apple-healthkit-privacy-questions-for-providers-developers/), which will be connected to some EHR systems, has drawn some concerns from health privacy experts because this consumer-turned enterprise technology hasn’t necessarily been built with HIPAA in mind. This isn’t to say that use of HealthKit can’t be HIPAA compliant, but the area is still new and the industry is still learning how these types of connected applications fit in from a privacy and security standpoint.

n his June 24 remarks on the [future of privacy and regulation](http://www.brookings.edu/events/2014/06/24-future-global-technology-privacy-regulation-brad-smith-microsoft), Microsoft General Counsel Brad Smith described how, by 2020, 50 billion devices will connected to networks around the world.  The exponential growth of data will ensure that privacy “is an issue that will continue to become more important.”

Turning to what this data-driven society means for privacy policy, Smith spoke about “how the two halves of this issue may come together” ― both “the relationship between citizens and between consumers and companies.”   He laid out “[four questions](http://www.youtube.com/watch?v=5GPB4Qs_WuU&feature=player_embedded#t=0)” ― a set of issues or principles ― that need to be addressed in both sectors to insure that both governments and technology “continue to serve people.”  These are (1) transparency, a right to know what information is collected and how it is used; (2) “appropriate control” over personal information; (3) accountability; and (4) international norms and collaboration.

Privacy in the Public and Private Spheres

Smith spoke about how these principles may operate differently in the public and private sectors.  For example, in the public sector, control belongs to “the public as a whole … through the rule of law” but, in the private sector, control should reside with individual consumers through mechanisms of “notice and consent and management.”  To this end, “companies should be accountable to regulators through regulation.  It needs to be well-designed regulation, it needs to be thoughtful, it needs to be balanced, but we cannot live in the Wild West when talking about information that is this important.”  In conversation, he said that legislation is “long overdue” and “I think and hope the Administration will send something to Congress” building on good information practices and principles in existing legislation.

## A Roadmap for Regulation

Transparency, control, and accountability are key elements of the Consumer Privacy Bill of Rights that was the centerpiece of the 2012 [White House privacy blueprint](http://www.whitehouse.gov/sites/default/files/privacy-final.pdf); international engagement is another key element of that blueprint.  The Consumer Privacy Bill of Rights was rooted in time-tested Fair Information Practice Principles updated to reflect the world of personal devices, social media, and new and evolving uses of data.  These same principles underlie the [protections federal agencies put in place](https://www.google.com/#q=dhs+fair+information+practice+principles) to control their use and management of data.

As the recent reports by the White House [Big Data](http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf) task force and [President's Council of Advisors on Science & Technology (PCAST)](http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf) found, reliance on notice and consent doesn’t work in a world of sensors and automated collection and places the burden on consumers rather than companies to manage privacy protection.  Brad Smith acknowledged this reliance is “under stress” because “everybody is asked so much to click” they simply do so “without reading.”  Thus, in a Big Data world,  other principles  ―  use, accountability, access to data that is collected ― take on much greater importance and require companies to be thoughtful stewards of information.   Even so, notice and consent have a role to play.  “We should not throw that principle overboard,” Smith said, because it is part of a right to control information.

## Status Quo Action – Surveillance Reform

USA Freedom Act, which is designed to reign in the NSA, passed the House in May. While this appears to present some general inherency problems, there is little reason to be concerned.

### -Many specific loopholes

Center for Democracy & Technology, June 26, 2014, https://cdt.org/blog/key-changes-needed-to-the-usa-freedom-act-h-r-3361/

Although introduced to prohibit bulk collection, the version of the USA FREEDOM Act passed by the House contains significant loopholes causing it to fall short of this objective.  These loopholes largely stem from last-minute [changes to the definition](http://justsecurity.org/10689/guest-post-support-usa-freedom-act" \t "_blank) of “Specific Selection Term” in Section 107 of the bill, which is key to the bill’s goal of requiring that surveillance target suspected wrongdoers.  Concerns over these changes were so strong that the bill [lost support](https://cdt.org/press/house-leadership-moves-to-gut-usa-freedom-act" \t "_blank) of a broad coalition of civil society advocates, many of America’s biggest tech companies, and half of the bill’s co-sponsors.  Specific problems with the revised definition are:

* *Excessive Ambiguity*:  The concept of “specific Selection Term” does not have a history of use in law, and the bill’s definition of “specific selection term” contains a non-exclusive a “such as” clause, which makes the term highly ambiguous and vulnerable to exploitation.
* *Potential Mass Collection*:  In light of the definition’s ambiguity and the lack of a narrow tailoring requirement, a specific selection term could encompass a major service provider or a large geographic region such as a city or state, thereby sweeping up millions of Americans in a single FISA order.  During a [June 5 Senate Intelligence Committee hearing](http://www.intelligence.senate.gov/hearings.cfm?hearingId=0cb5dc5497c5ffb2985cb30c4755265f" \t "_blank), Chairman Diane Feinstein suggested that the definition is broad enough that it might be used to obtain all flight manifests of an entire airline.
* *Loopholes in New Terms*: “Address” and “device” were added to the definition as examples of specific selection terms, but with loopholes that could permit mass collection.  For example, if “address” is read as an IP address block, or if “device” is read as a large-scale router, a single order could encompass the data of thousands of individuals.
* *FISC Disclosures Are Not Sufficient*:  The bill’s requirement – in Sec. 401 – that the FISC publicly disclose important interpretations of law is not sufficient to prevent exploitation of the bill’s ambiguities.  The bill gives the Office of the Director of National Intelligence discretion to redact these rulings, or to publicly release them in a summary form.  This could lead to vague disclosures which fail to alert the public whether the FISC has interpreted Specific Selection Term in a highly broad manner to facilitate mass collection. While the declassification of significant opinions is an important reform, it cannot be relied on to effectively end bulk collection.

### -Even if legislation passes (a big if), it won’t reign in foreign intelligence surveillance will contain many loopholes

Politico, July 17, 2014, http://dyn.politico.com/printstory.cfm?uuid=7852F361-3A87-4261-A560-3A4F49A876A2

Surveillance reformers on Capitol Hill are up against a wall — and short on time.

The USA Freedom Act, the Hill’s preeminent measure to curb NSA authority in the wake of Edward Snowden’s leaks, cleared the House and has been waiting to see movement in the Senate as advocates in and out of Congress try to navigate a tough negotiating landscape. Privacy advocates and intelligence hawks primarily disagree over how best to end the government’s bulk phone records program.

But a diminishing resource in an election year may be an even bigger factor as to whether anything gets done on that and other surveillance questions — the calendar. Lawmakers won’t be around the Beltway in August, and much of the Senate will be in full-on election mode by September.

That reality isn’t lost on the bill’s supporters. Senate Judiciary Chairman Patrick Leahy (D-Vt.), the measure’s top sponsor in the upper chamber, is considering an attempt to bring the bill straight to the Senate floor. The Judiciary Committee has held several hearings on surveillance reforms this Congress but hasn’t yet scheduled a markup.

Leahy “has been calling for these reforms for years and is working to ensure the Senate seizes on this historic opportunity to pass real reform this work period,” one of his aides said.

Majority Leader Harry Reid (D-Nev.) doesn’t have a floor plan for the surveillance bill yet, a Senate leadership aide said last week. While surveillance reform has become a higher-profile issue since the White House endorsed major changes to its call records program in January, Reid also is facing pressing debates on highway funding and the Export-Import Bank — not to mention supporting his Democratic colleagues trying to retain their seats in a tough election year. Add in a desire for a legislative fix to the Supreme Court’s *Hobby Lobby* decision, and the surveillance timeline becomes more narrow.

“That’s a good question, and I can’t really tell you,” Senate Intelligence Chairwoman Dianne Feinstein (D-Calif.) said when asked about the bill’s chances to clear the Senate this year.

The main focus for negotiators on Capitol Hill, in the administration and among privacy advocates remains how the bill ends the government’s bulk phone records program — the subject of the first Snowden stories last summer. The measure would allow the government to ask phone companies for call records relevant to particular investigations, rather than automatically receiving all the records generated each day. But privacy advocates contend — and some lawmakers concur — that the legislative approach used in the bill won’t actually stop the government from getting information on more Americans than it needs.

Would-be reformers have a tough needle to thread: The White House and NSA defenders in Congress already support the current language. That means there’s little room to strengthen the measure’s protection against bulk collection and still keep the intelligence community happy.

As Senate aides and lawmakers grapple with the pending bill, discussions also continue outside of Congress. Civil liberties groups and the White House have engaged each other more directly than during House negotiations in May, meeting to debate the bill last week, according to a source familiar with the discussion.

“The administration supports the USA Freedom Act, but is willing to work on specific modifications to the House-passed bill,” White House spokeswoman Caitlin Hayden said in a statement. She declined to provide specifics.

Separately, the NSA’s communications content collection programs have gotten more attention in the past several weeks, including a surprising House vote on an appropriations amendment that bans funding from being used to search its databases for American data without a warrant — or what critics call the “backdoor search loophole.”

“I am going to try to close the backdoor search loophole on every possible relevant vehicle, and I’m quite certain Sen. [Mark] Udall and Sen. [Rand] Paul and many others will all be part of a very significant bipartisan effort,” said Sen. Ron Wyden (D-Ore.).

That will not be a quick fix. The Senate amendments process has been tightly controlled by leadership this year, and while reforms of the relevant statute — section 702 of the Foreign Intelligence Surveillance Act — are certainly on the minds of privacy hawks, the main focus for privacy groups and many lawmakers remains ending bulk data collection. Plus, Appropriations Committee Chairwoman Barbara Mikulski (D-Md.) is unlikely to back major changes to Foreign Intelligence Surveillance Act programs.

Ultimately, the landscape reflects the tall task of striking harmony between privacy hawks and national security hard-liners. Even if civil liberties-minded senators could get a more aggressive reform bill through the upper chamber over the objections of NSA defenders, it’d be a long shot to win favor from the administration or in the House.

There’s no end-of-the-year deadline forcing lawmakers to act this Congress, but advocates want to capitalize on momentum from Snowden’s leaks and the president’s NSA speech. And NSA defenders may feel pressure to act this year before negotiations bleed into the June 2015 expiration of authority for the agency’s current call detail records program.

### -Even if legislation passes as-is, it won’t contain a privacy advocate on the FIS court

Time, July 10, 2014, <http://time.com/2970766/privacy-freedom-act-reform-secret-nsa-oversight-fisa/>

The version of the USA FREEDOM Act that [passed](http://www.samachar.com/bill-curbing-nsa-passes-house-as-advocates-demand-more-ofwxO9igjbh.html" \t "_blank) in the House in May—which stirred controversy after civil liberties groups dropped support for the watered down legislation in droves—largely eliminated the special advocate position, replacing it instead with an official to consult in case of novel legal situations. The version of the bill championed by Senator Patrick Leahy, a Vermont Democrat, and under consideration in the Senate Judiciary Committee, includes a special advocate who would permanently represent privacy interests on the court.

The secrecy of proceedings in the highly-classified FISC and the question of declassification has been another major point of contention. “The House-passed version of the bill has enormous loopholes to that requirement,” said ACLU Legislative Counsel Neema Singh Guliani.

### -The bill may not end all authorities for metadata collection

Kate Martin, July 17, 2014, http://justsecurity.org/12970/guest-post-usa-freedom-act/

* When the House passed the [USA Freedom Act](https://beta.congress.gov/113/bills/hr3361/BILLS-113hr3361eh.pdf) (H.R. 3361) in May,  both [Members](http://judiciary.house.gov/index.cfm/2014/5/goodlatte-conyers-sensenbrenner-scott-nadler-and-forbes-applaud-house-passage-of-the-usa-freedom-act) and the [administration](http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr3361h_20140521.pdf) announced that it would end bulk collection of metadata about Americans’ communications.  The [administration is now urging Congress](http://www.dni.gov/files/documents/As%20Delivered%20PDDNI%20SSCI%20Opening%20Remarks_Jun_5_2014.pdf) to pass the bill as soon as it can and [Senators are now considering](http://www.intelligence.senate.gov/hearings.cfm?hearingId=0cb5dc5497c5ffb2985cb30c4755265f) revisions to specific language in the House-passed bill.
* But the administration is still withholding key information that is needed before any Member of Congress or the public can have confidence that the USA Freedom Act would in fact limit all the authorities that the Department of Justice claims can be used for the NSA’s bulk collection of telephone metadata.
* The bill passed by the House amends section 501 of the Foreign Intelligence Surveillance Act (sometimes called section 215) to prohibit the bulk collection of telephone metadata and require instead the use of a “specific selection term” to identify metadata sought by the government.  The Senate is currently working on revisions to the definition of “specific selection term.”  (The House bill would also amend the [FBI’s authority to use National Security Letters](http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap121-sec2709.pdf) to obtain “toll billing records information.”)
* But we don’t know whether the Justice Department has opined that other statutory authorities – not now addressed in the USA Freedom Act – could authorize the NSA’s bulk collection.  Without this knowledge, we can’t be certain whether the proposed amendments to section 501 (215) will in fact be sufficient to prohibit the NSA from engaging in bulk collection of metadata using some other hitherto unidentified authority.
* This is not a fanciful concern.  There is in fact a still partly secret OLC opinion by the Justice Department that may address precisely this question.  As readers know, the bulk metadata collection program started before the FISA court issued its first 2006 order authorizing the program under section 501.  The Justice Department has disclosed that in May 2004, the OLC issued an[opinion](http://www.justice.gov/olc/docs/memo-president-surveillance-program.pdf) entitled:  “[Memorandum Regarding Review of the Legality of the [President’s Surveillance] Program](http://www.justice.gov/olc/olc-foia1.htm).”  Parts of that 2004 Memorandum discussing the warrantless acquisition of the contents of Americans’ communications were declassified and released in 2011.  But at the time, the government had refused to acknowledge the existence of the bulk metadata surveillance and much of OLC memo, which apparently discussed authority for bulk collection, was blacked out.
* Since the [December 2013 official declassification](http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/991-dni-announces-the-declassification-of-the-exisitence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11,-2001) of the fact that the bulk metadata collection pre-dated the court’s 2006 orders under section 501(215),  Members of the Senate and the [Center for National Security Studies](http://www.cnss.org/resources.php/185/CNSS%20Letter%20to%20the%20Obama%20Administration%20Seeking%20Declassification%20of%20Domestic%20Surveillance%20Authorities) have pressed for a new review and release of the 2004 OLC Memo that discusses any other potential authorities for bulk metadata collection.   At her nomination hearing to be CIA General Counsel, Senator Wyden [asked](http://www.intelligence.senate.gov/131217/krasspost.pdf) (see p. 5-6 in link) the then Principal Deputy Attorney General for the Office of Legal Counsel whether the opinion addressed bulk telephone metadata collection and if so, whether the OLC relied “at that time on a statutory basis other than the Foreign Intelligence Surveillance Act for the authority to conduct bulk telephony metadata collection?” Wyden was told that the opinion was still classified but that further classification review of the opinion would be appropriate.

### -Surveillance could potentially expand if the cybersecurity bill passes

[**The Verge**](mailto:http://www.theverge.com/2014/7/9/5881691/congress-will-vote-on-CISA-controversial-cybersecurity-bill), July 9, 2014

There's a new cybersecurity bill making its way through Congress, sponsored and written by Diane Feinstein (D-CA), and critics are already calling it a new backdoor for surveillance by the National Security Agency. The Cybersecurity Intelligence Sharing Act of 2014 (CISA) was [approved by the Senate Intelligence Committee](http://www.feinstein.senate.gov/public/index.cfm/press-releases?ContentRecord_id=4c0ee3f0-8191-410c-b35d-bfe3bb0b3b46" \t "_blank) yesterday, putting it on track for a Senate vote this summer. But like [its controversial predecessors](http://www.theverge.com/2013/10/21/4863734/feinstein-working-on-new-cispa-cyberthreat-bill-curb-privacy-concerns), the bill is coming under fire as a step backwards in the fight for surveillance reform.

The bill's primary effect would be a new requirement for sharing information on "cyber threat indicators," a vague term that could refer to anything from an ongoing hack to a vulnerability in commercial software. Once a company makes a report to the government with information about a threat indicator, CISA would require broad sharing across federal agencies, including with the NSA, which would be given a more central role in threat management under the new scheme. Companies would also be encouraged to monitor their networks to gather more information about the threat.

Advocacy groups have seized on the reporting requirements as a troubling expansion of NSA access to private networks. The Center for Democracy in Technology [says the provision](https://cdt.org/insight/analysis-of-feinstein-chambliss-cybersecurity-information-sharing-act-of-2014/" \t "new) "risks turning the cybersecurity program it creates into a back door wiretap." CDT also notes the bill lacks many crucial privacy protections that were included in previous cybersecurity acts. The Electronic Frontier Foundation [calls the bill](https://www.eff.org/deeplinks/2014/06/zombie-bill-comes-back-look-senates-cybersecurity-information-sharing-act-2014" \t "new) "fatally flawed," and raised concerns that it would create a new pipeline of data from independent companies to the NSA.

### -Privacy groups have withdrawn support for the House version

The Hill, June 19, 2014, <http://thehill.com/policy/technology/209898-privacy-groups-threaten-to-oppose-senate-nsa-bill>

Thirty-eight privacy and tech groups are warning Senate leadership that they will oppose a Senate reform bill if it doesn’t go far enough to end sweeping surveillance programs at the National Security Agency (NSA).

“Unless the version of the USA Freedom Act that the Senate considers contains substantial improvements over the House-passed version, we will be forced to oppose the bill that so many of us previously worked to advance,” the groups said in a letter on Wednesday.

Signatories include the American Civil Liberties Union, Reddit, the Center for Democracy and Technology, Access and the New America Foundation’s Open Technology Institute.

The letter comes as the Senate takes up the USA Freedom Act — a bill to end the NSA’s “bulk” surveillance programs and make other changes within the intelligence community — that was introduced by Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) and Patriot Act author Rep. Jim Sensenbrenner (R-Wis.) last year.

In May, the House passed a compromise version of the bill.

While privacy advocacy groups initially supported the bill, they withdrew their support as the bill headed to the House floor, saying it had been “watered down” through eleventh-hour negotiations with the administration and House leadership.

In their Wednesday letter, the groups warn the Senate not to follow the House’s example and threaten to oppose a weak reform bill.

The groups asked that the Senate NSA reform bill, among other things, “definitively end ‘bulk’ collection,” increase transparency around U.S. surveillance and reform the Foreign Intelligence Surveillance Court, which approves government surveillance requests.

“We believe that strong legislation can effectively address our concerns and we are committed to supporting Congress in passing such legislation,” the letter said, “but we will be forced to oppose any bill that is not a substantial improvement over the version of the USA Freedom Act that was passed in the

## Status Quo Action – Consumer Privacy

### -No movement for consumer privacy protection now

The Hill, June 26, 2014, http://thehill.com/policy/technology/210677-lofgren-no-appetite-for-consumer-privacy-bill

Rep. Zoe Lofgren (D-Calif.) doesn’t see Congress moving a bill to protect consumer privacy anytime soon.

“We’re not doing that,” Lofgren said Thursday.

arlier this year, the administration [renewed](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CDEQFjAA&url=http%3A%2F%2Fthehill.com%2Fpolicy%2Ftechnology%2F204961-white-house-big-data-report-calls-for-new-privacy-laws&ei=tjusU6H4NMnZ8AH6vICwAg&usg=AFQjCNGKsDhfmeZ2u421lPtp3cDUOY4GPw&bvm=bv.69837884,d.b2U" \t "_blank) those calls for legislation through its report on Big Data.

That report — initiated after the administration faced public backlash over government surveillance practices — called on the Commerce Department to work with the private sector to develop legislative proposals.

But Lofgren said Thursday that there is no enthusiasm in Congress for such a bill at the moment.

“Do you see any appetite to do that? No,” she said.

That appetite might increase based on consumer reactions to evolving, and potentially privacy-threatening, technologies, she acknowledged.

“Consumer reaction … will shape what goes on,” she said, speaking at an event on mobile technology hosted by Politico.

For now, Congress is focused on privacy from government surveillance she said, stressing that privacy from governments and privacy from companies are different issues.

“People have an interest in privacy overall, but Yahoo can’t arrest you,” she said.

She pointed to a [House vote](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QqQIwAA&url=http%3A%2F%2Fthehill.com%2Fpolicy%2Ftechnology%2F210138-nsa-critics-hail-votes-as-game-changer&ei=xTusU4voOMiV8AGax4GQBA&usg=AFQjCNE1JWUxRmyudIQLaXNxMZHtFS6Fjg&bvm=bv.69837884,d.b2U" \t "_blank) last week that overwhelmingly approved an amendment to the Defense Department’s funding bill that will require the National Security Agency to obtain a warrant before searching its databases for information about people in the United States.

Rep. Jason Chaffetz (R-Utah), who appeared on Thursday’s panel with Lofgren, also stressed the need for privacy protections for U.S. users, whose information is swept up by government surveillance programs.

Deciding to use a tech company’s product or service “doesn’t mean that you are also giving permission for the federal government to follow you and tap into your life,” Chaffetz said.

## Advantage Areas

Privacy/totalitarianism. The privacy and totalitarianism risks associated with state surveillance are considerable.

Former debater Glenn Greenwald, who was instrumental in breaking the Snowden story and also in past efforts to criticize US surveillance efforts under the PATRIOT Act, argues that the objective of NSA surveillance is the [elimination of global privacy](http://rt.com/usa/glenn-greenwald-reddit-nsa-600/).

Extensive surveillance is a problematic assault on privacy not only because it collects individual data regarding what a user is doing at a particular point but also, and more importantly, because extensive data collection makes it possible to develop an entire profile of a person. This could both discourage a person from speaking freely and also discourage him or her from associating with particular people.

**Citron & Macht, 2013,**Danielle Keats Citron, Lois K. Macht Research Professor of Law, University of Maryland School of Law; Affiliate Scholar, Stanford Center on Internet and Society; Affiliate Fellow, Yale Information Society Project., David Gray, Associate Professor of Law, University of Maryland School of Law. We are grateful to Neil Richards for his thoughtful essay and feedback and to Julie Cohen, Leslie Henry, Amanda Pustilnik, Daniel Solove, and the participants in the Harvard Law Review Symposium on Privacy and Technology for their helpful suggestions, “ADDRESSING THE HARM OF TOTAL SURVEILLANCE: A REPLY TO PROFESSOR NEIL RICHARDS,” May, p. 270

The **continuous and indiscriminate surveillance** they accomplish **is damaging because it violates reasonable expectations of quantitative privacy, by which we mean privacy interests in large aggregations of information** that are independent from particular interests in constituent parts of that whole. To be sure, the harms that Richards links to intellectual privacy are very much at stake in recognizing a right to quantitative privacy. But rather than being a function of the kind of information gathered, we think that **the true threats to projects of self-development and democratic culture lie in the capacity of new and developing technologies to facilitate a surveillance state.**In adopting this view, we ally ourselves in part with commitments to a quantitative account of Fourth Amendment privacy promoted by at least five Justices of the Supreme Court last Term in United States v. Jones.  In Jones, police officers investigating drug trafficking in and around the District of Columbia attached a GPS-enabled tracking device on defendant Jones's car. By monitoring his movements over the course of a month, investigators were able to document both the patterns and the particulars of his travel, which played a critical role in his ultimate conviction. Although the Court resolved Jones on the narrow grounds of physical trespass, five justices wrote or joined concurring opinions showing sympathy for the proposition that citizens hold reasonable expectations of privacy in large quantities of data, even if they lack reasonable expectations of privacy in the constitutive parts of that whole. Thus, they would have held that Jones had a reasonable expectation in the aggregate of data documenting his public movements over the course of four weeks, even though he did not have any expectation of privacy in his public movements on any particular afternoon.  The account of quantitative privacy advanced by the Jones concurrences has much in common with the views promoted by Warren and Brandeis. Specifically, the concurring Justices in Jones expressed worry that **by "making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track," programs of broad and indiscriminate surveillance will "chill[] associational and expressive freedoms," and "alter the relationship between citizen and government in a way that is inimical to a democratic society**." Their concerns are well-grounded in original understandings of the Fourth Amendment. **As Professor William Stuntz has shown, the Fourth Amendment was drafted partly in reaction to eighteenth-century cases involving the British government's use of general warrants to seize personal diaries and letters in support of seditious-libel prosecutions that were designed to suppress political thought. Despite these roots, quantitative privacy is just beginning to receive recognition because it is only now under threat of extinction by technologies like Virtual Alabama and fusion centers.**

Beyond individual privacy violations, this surveillance laws the foundations for totalitarianism.  Surveillance totalitarianism possible by discouraging intellectual exploration of controversial ideas and creating a power relationship between the government and the subject who is subject to surveillance.

Neil**Richards, 2013,**law professor,Washington University School of Law, Harvard Law Review, PRIVACY AND TECHNOLOGY: THE DANGERS OF SURVEILLANCE, p. 1934

From the Fourth Amendment to George Orwell's Nineteen Eighty-Four, and from the Electronic Communications Privacy Act to films like Minority Report and The Lives of Others, **our law and culture are full of warnings about state scrutiny of our lives.** These warnings are commonplace, but they are rarely very specific. Other than the vague threat of an Orwellian dystopia, as a society we don't really know why surveillance is bad and why we should be wary of it. To the extent that the answer has something to do with "privacy," we lack an understanding of what "privacy" means in this context and why it matters. We've been able to live with this state of affairs largely because the threat of constant surveillance has been relegated to the realms of science fiction and failed totalitarian states **But these warnings are no longer science fiction. The digital technologies that have revolutionized our daily lives have also created minutely detailed records of those lives**. In an age of terror, our government has shown a keen willingness to acquire this data and use it for unknown purposes. We know that governments have been buying and borrowing private-sector databases,  and **we recently learned that the** National Security Agency (**NSA) has been building a massive data and supercomputing center in Utah, apparently with the goal of intercepting and storing much of the world's Internet communications for decryption and analysis**.  Although we have laws that protect us against government surveillance, secret government programs cannot be challenged until they are discovered. And even when they are, **our law of surveillance provides only minimal protections. Courts frequently dismiss challenges to such programs for lack of standing, under the theory that mere surveillance creates no harms.** The Supreme Court recently reversed the only major case to hold to the contrary, in Clapper v. Amnesty International USA, finding that the respondents' claim that their communications were likely being monitored was "too speculative."  But the important point is that our society lacks an understanding of why (and when) government surveillance is harmful. Existing attempts to identify the dangers of surveillance are often unconvincing, and they generally fail to speak in terms that are likely to influence the law. In this Article, I try to explain the harms of government surveillance. Drawing on law, history, literature, and the work of scholars in the emerging interdisciplinary field of "surveillance studies," I offer an account of what those harms are and why they matter. I will move beyond the vagueness of current theories of surveillance to articulate a more coherent understanding and a more workable approach. At the level of theory, I will explain why and when surveillance is particularly dangerous and when it is not. First, **surveillance is harmful because it can chill the exercise of our civil liberties**. With respect to civil liberties**, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas**. To protect our intellectual freedom to think without state oversight or interference, we need what I have elsewhere called "intellectual privacy." **A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance.** At a practical level, I propose a set of four principles that should guide the future development of surveillance law, allowing for a more appropriate balance between the costs and benefits of government surveillance. First, we must recognize that surveillance transcends the public/private divide. Public and private surveillance are simply related parts of the same problem, rather than wholly discrete. Even if we are ultimately more concerned with government surveillance, any solution must grapple with the complex relationships between government and corporate watchers. Second, we must recognize that secret surveillance is illegitimate and prohibit the creation of any domestic-surveillance programs whose existence is secret. Third, we should recognize that total surveillance is illegitimate and reject the idea that it is acceptable for the government to record all Internet activity without authorization. **Government surveillance of the Internet is a power with the potential for massive abuse.** Like its precursor of telephone wiretapping, it must be subjected to meaningful judicial process be-fore it is authorized. We should carefully scrutinize any surveillance that threatens our intellectual privacy. Fourth, we must recognize that **surveillance is harmful. Surveillance menaces intellectual privacy and increases the risk of blackmail, coercion, and discrimination; accordingly, we must recognize surveillance as a harm in constitutional standing doctrine**. Explaining the harms of surveillance in a doctrinally sensitive way is essential if we want to avoid sacrificing our vital civil liberties.

Jonathan Schell, writing in the [September 4th issue of Nation](http://www.thenation.com/article/176032/edward-snowden-and-chelsea-manning-new-dissidents), argues that this is more power than Stalin was able to exercise in totalitarian Russia.

And certainly, the four Poles, of all people, are as fully aware as any sensible person of the abyss of difference that separates the Obama administration from, say, the regime of Joseph Stalin, slayer of tens of millions of his own people. And **yet it is chillingly true**at the same time **that the US government has gone further than any previous government—not excluding Stalin’s—in setting up machinery that satisfies certain tendencies that are in the genetic code of totalitarianism. One is the ambition to invade personal privacy without check or possibility of individual protection. This was impossible in the era of mere phone wiretapping, before** the recent explosion of electronic communications—before the **cellphones that disclose the whereabouts of their owners, the personal computers with their masses of personal data and easily penetrated defenses, the e-mails that flow through readily tapped cables and servers**, the biometrics, the street-corner surveillance cameras. But now, to borrow the name of an intelligence program from the Bush years, “Total Information Awareness” is technologically within reach. The Bush and Obama administrations have taken giant strides in this direction. That China and Russia—and Britain, and many other countries—have done the same is hardly comforting to the humble individual under the eye of the universal spying apparatus. **A second totalitarian tendency has been the ambition to control the entire globe**—a goal built into fascist as well as communist ideologies of the early twentieth century. **In Hannah Arendt’s words, “Evidence that totalitarian governments aspire to conquer the globe and bring all countries on earth under their domination can be found repeatedly in Nazi and Bolshevik literature**.” Neither achieved it, or even came close. But now, in the limited arena of information, a sort of shadow or rudiment of this ambition is near realization by the “sole superpower,” the United States**. Much attention has been paid to Americans’ loss of privacy rights, but relatively overlooked in the debate over the government’s surveillance activities**(at least in the United States) **has been that all foreign communications—including those occurring in the lands of close allies, such as Germany—are fair game and are being swept into the US data banks.** The extent of the US global reach over information was mirrored in Snowden’s fate. Astonishingly, almost no fully democratic country would have him. (The conspicuous exception was Bolivia, whose president suffered the indignity of a forced diversion and landing of his plane when he was suspected of carrying Snowden to safety.) Almost all others, including Poland, bowed to US pressure, actual or potential, to refuse Snowden protection. The Polish letter writers were scandalized by this spectacle. “The fact that only dictatorial governments agreed to give him shelter shames the democratic states,” they wrote. “Our democracies discredit themselves with their indifference and cowardice in this matter.” What happened to Snowden in Moscow diagramed the new global reality. He wanted to leave Russia, but the State Department, in an act of highly dubious legality, stripped him of his passport, leaving him—for purposes of travel, at least—stateless. Suddenly, he was welcome nowhere in the great wide world, which shrank down to a single point: the transit lounge at Sheremetyevo. Then, having by its own action trapped him in Russia, the administration mocked and reviled him for remaining in an authoritarian country. **Only in unfree countries was Edward Snowden welcome. What we are pleased to call the “free world” had become a giant prison for a hero of freedom.**

The NSA doesn’t have a great track record when it comes to limiting abuse of its authority.  During the Vietnam war, [the NSA spied on Mohammed Ali, Martin Luther King, and Senator Howard Baker](http://www.madcowprod.com/2013/10/04/drug-trafficking-the-nsa-the-crash-of-cocaine2/).  Arab American lawyer [Abdeen Jabara was also spied on](http://mondoweiss.net/2013/10/american-lawyer-spied.html). In March, 2013, the NSA program, Boundless Informant, collected 97 billion pieces of metadata.  From 1940 to 1973, the CIA and FBI engaged in a covert mail opening program.  The Army intercepted domestic radio communications. Any Army surveillance program placed more than 100 people under surveillance.

Although the internal link to totalitarianism from the collection of individual information by private companies is inherently smaller, there are massive privacy violations, and since governments can get ahold of the information, there is a link into totalitarianism

[Daily Mail,](mailto:http://www.dailymail.co.uk/news/article-2651145/Young-people-wary-giving-privacy-online-read-1984.html) July 7, 2014:

Noel Sharkey, a professor of artificial intelligence and robotics at Sheffield University, said that older people were more cautious with their personal data. Addressing the Cheltenham Science Festival, he said: 'I'm 65, I don't want to be targeted. I am very uncomfortable with it. It seems to me our privacy is gradually being violated and eroded without us noticing. 'I am part of the generation which all read 1984 - I think we are less happy about giving up our privacy. 'But the younger generation aren't really thinking about it. The services that Google and Facebook give us are so good that people are willing to trade off their privacy for them.' He said Google's recording of all our online activities meant it knew far too much about us. He added: 'At the moment it doesn't seem harmful. But because governments can get hold of this information, they can monitor you, things might change quite dramatically.' Google has invested billions of pounds buying up cutting-edge technologies which will increase their access to people's information. The internet giant recently paid £1.9billion for Nest Labs, a firm which makes internet-connected heating systems, allowing people to control their thermostats from afar. Supporters argue that having greater control over home applications - which may soon include fridges that automatically reorder when you run out of food and lighting systems that turn on when they sense your approach - can only benefit consumers. But connecting more things to the internet enables large firms to collect more and more data.

Racism. Many argue that NSA surveillance is illegitimately targeted at minorities, particularly Arab and Muslim minorities. In July of this year (2014), the [Intercept](mailto:https://firstlook.org/theintercept/article/2014/07/09/under-surveillance/), Glenn Greenwald’s new website, published the email addresses of more than 7,000 Muslim Americans who are under warrantless surveillance

The National Security Agency and FBI have covertly monitored the emails of prominent Muslim-Americans—including a political candidate and several civil rights activists, academics, and lawyers—under secretive procedures intended to target terrorists and foreign spies. According to documents provided by NSA whistleblower Edward Snowden, the list of Americans monitored by their own government includes:

• Faisal Gill, a longtime Republican Party operative and one-time candidate for public office who held a top-secret security clearance and served in the Department of Homeland Security under President George W. Bush;

• Asim Ghafoor, a prominent attorney who has represented clients in terrorism-related cases;

• Hooshang Amirahmadi, an Iranian-American professor of international relations at Rutgers University;

• Agha Saeed, a former political science professor at California State University who champions Muslim civil liberties and Palestinian rights;

• Nihad Awad, the executive director of the Council on American-Islamic Relations (CAIR), the largest Muslim civil rights organization in the country.

The individuals appear on an NSA spreadsheet in the Snowden archives called “FISA recap”—short for the Foreign Intelligence Surveillance Act. Under that law, the Justice Department must convince a judge with the top-secret Foreign Intelligence Surveillance Court that there is probable cause to believe that American targets are not only agents of an international terrorist organization or other foreign power, but also “are or may be” engaged in or abetting espionage, sabotage, or terrorism. The authorizations must be renewed by the court, usually every 90 days for U.S. citizens.

The spreadsheet shows 7,485 email addresses listed as monitored between 2002 and 2008. Many of the email addresses on the list appear to belong to foreigners whom the government believes are linked to Al Qaeda, Hamas, and Hezbollah. Among the Americans on the list are individuals long accused of terrorist activity, including Anwar al-Awlaki and Samir Khan, who were killed in a 2011 drone strike in Yemen.

This racism advantage is unique to the government surveillance Affirmative cases. Although it is possible that mass surveillance conducted by private companies may be done in a racially inappropriate manner, these companies are really just trying to collect all of the information that they can on absolutely everyone.

Economy. This advantage is also specific to the government surveillance case area. The argument is that foreign companies and countries no longer want to do business with US internet companies because information on their citizens is turned over to and held by the NSA.

[Arvind Ganesan](mailto:http://globalpublicsquare.blogs.cnn.com/2013/07/15/how-the-nsa-scandal-hurts-the-economy/) wrote on CNN’s website on July 13, 2013:

The National Security Agency surveillance scandal has been devastating to the U.S. government’s credibility as an advocate for Internet freedom. But the impact on U.S. technology companies and a fragile American economy may be even greater.

Every new revelation suggests far more surveillance than imagined and more involvement by telephone and Internet companies, with much still unknown. One of the most troubling aspects of this spying is that foreign nationals abroad have no privacy rights under U.S. law. Foreigners using the services of global companies are fair game. (There is also a certain irony to the revelations, considering that some European governments such as Germany and the Netherlands are [strong U.S. allies on Internet freedom](http://www.humanrights.gov/2012/11/20/fact-sheet-freedom-online-coalition/) but may simultaneously be targets of U.S. surveillance online.)

A July 1 report by *Der Spiegel* on the NSA [spying](http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html) on European officials infuriated governments a week before negotiations started on a massive U.S.-European Union trade agreement that could be [worth](http://www.whitehouse.gov/photos-and-video/video/2013/06/17/president-obama-makes-statement-transatlantic-trade-and-investment#transcript) almost $272 billion for their economies and 2 million new jobs. Officials throughout Europe, most notably French President Francois Hollande, said that NSA spying [threatens](http://www.nytimes.com/2013/07/02/world/europe/france-and-germany-piqued-over-spying-scandal.html?ref=world) trade talks.

The French government unsuccessfully [called](http://www.businessweek.com/ap/2013-07-03/france-calls-for-2-week-delay-in-us-eu-trade-talks) for a two-week postponement of the trade talks. The next day, it had to address [allegations](http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441631_3224.html) in *Le Monde* of its own domestic mass surveillance program.

For the Internet companies [named](http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/) in reports on NSA surveillance, their bottom line is at risk because European markets are crucial for them. It is too early assess the impact on them, but the stakes are clearly huge. For example, Facebook has about [261 million active monthly European users](http://files.shareholder.com/downloads/AMDA-NJ5DZ/2297890522x0x631721/fc91bd68-c60f-46c0-b3d4-f26455e115f7/FB_Q412_InvestorDeck.pdf), compared with about 195 million in the U.S. and Canada, and [22%](http://investor.apple.com/secfiling.cfm?filingID=1193125-13-168288&CIK=320193) of Apple’s net income came from Europe in the first quarter of 2013.

Europe was primed for a backlash against NSA spying because people care deeply about privacy after their experience of state intrusion in Nazi Germany and Communist Eastern Europe. And U.S. spying on Europeans via companies had been a simmering problem since at least 2011.

In June 2011, Microsoft [admitted](http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225) that the United States could bypass EU privacy regulations to get vast amounts of cloud data from their European customers. Six months later, BAE Systems, based in the United Kingdom, [stopped](http://www.zdnhttp/www.computerweekly.com/news/2240112018/Office365-fails-BAes-legal-teamet.com/blog/london/defense-giant-ditches-microsofts-cloud-citing-patriot-act-fears/1349) using the company’s cloud services because of this issue.

A major [EU survey](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf) released in June 2011 found that “[t]hree out of four Europeans accept that revealing personal data is part of everyday life, but they are also worried about how companies – including search engines and social networks – use their information.” Only 22% trusted e-mail, social networking, and search companies with their data.

Then the [European Parliament issued a report](http://www.europarl.europa.eu/committees/en/libe/studiesdownload.html?languageDocument=EN&file=79050) on privacy in October 2012 confirming Microsoft’s claim and urging new privacy protections between the EU and the United States. The EU tried, but the [*Financial Times* reported](http://www.ft.com/intl/cms/s/0/42d8613a-d378-11e2-95d4-00144feab7de.html#axzz2XU1yx8Ow) that senior Obama administration officials and tech industry representatives successfully lobbied against it.

The NSA scandal has brought tensions over spying to a boil. German prosecutors [may open a criminal investigation](http://www.spiegel.de/international/germany/german-prosecutors-to-review-nsa-spying-allegations-a-908636.html) into NSA spying. On July 3, Germany’s interior minister [said](http://hosted2.ap.org/APDEFAULT/495d344a0d10421e9baa8ee77029cfbd/Article_2013-07-03-EU-Germany-NSA-Surveillance/id-9172c3109bd7495d8d4dd3d8225f9742) that people should stop using companies like Google and Facebook if they fear the U.S. is intercepting their data. On July 4, the European Parliament condemned spying on Europeans and [ordered](http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//EN&language=EN) an investigation into mass surveillance. The same day, Neelie Kroes, the EU’s chief telecom and Internet official, [warned](http://europa.eu/rapid/press-release_MEMO-13-654_en.htm?locale=en) of “multi-billion euro consequences for American companies” because of U.S. spying in the cloud.

The companies have belatedly distanced themselves from the NSA and called for more transparency. Google, Microsoft, Yahoo and Facebook are in a particularly tough spot as members of the [Global Network Initiative](http://globalnetworkinitiative.org/), a group (including Human Rights Watch) formed to verify whether companies respect freedom of expression and privacy online

Foreign Relations. Once again, this advantage is specific to the foreign surveillance area. Many countries are upset that their citizens and governments are being spied on.

-- Germany

[Bloomberg](mailto:http://www.bloomberg.com/news/2014-07-11/u-s-seeks-to-mend-german-relations-after-spy-expelled.html), July 11, 2014

President [Barack Obama](http://topics.bloomberg.com/barack-obama/)’s administration lavished praise on its partnership with Germany while sidestepping specifics of espionage allegations that led to the expulsion of the top American intelligence officer in Berlin. “We’re in touch because we recognize the value and the strong partnership that exists between the United States and Germany,” White House press secretary [Josh Earnest](http://topics.bloomberg.com/josh-earnest/) told reporters yesterday. The administration must move quickly beyond such reassuring words to avoid damaging trans-Atlantic trade talks, business deals and national-security priorities, including talks on Iran’s nuclear program and sanctions against Russia for its role in Ukraine, according to foreign-policy specialists. “There are high stakes,” Jeffrey Anderson, head of a German-European studies center at Georgetown University in Washington, said in an interview. “There are plenty of areas where we need to work with the Germans, or where we can, and all this is getting sidetracked.” The damage is potentially long-term, Anderson said. “It’s implanted seeds of mistrust, disappointment and betrayal that are going to take a long time to uproot.” The efforts may intensify within days. Secretary of State John Kerry may meet his German counterpart, Frank-Walter Steinmeier, at talks in Vienna on curbing [Iran](http://topics.bloomberg.com/iran/)’s nuclear ambitions. Secretary of State John Kerry, right, may meet his German counterpart, Frank-Walter... [Read More](http://www.bloomberg.com/news/2014-07-11/u-s-seeks-to-mend-german-relations-after-spy-expelled.html) “I would expect that Secretary Kerry and Foreign Minister Steinmeier will have an opportunity to speak sometime in the coming days, and I would just reiterate that our relationship with Germany is extremely important,” State Department spokeswoman Jen Psaki told reporters in Washington yesterday. “We have many areas we work together on.”

* Many countries

[Deb Riechman](mailto:http://bigstory.ap.org/article/nsa-spying-threatens-hamper-us-foreign-policy) wrote on October 26, 2013

Secretary of State John Kerry went to Europe to talk about Mideast peace, Syria and Iran. What he got was an earful of outrage over U.S. snooping abroad. President Barack Obama has defended America's surveillance dragnet to leaders of Russia, Mexico, Brazil, France and Germany, but the international anger over the disclosures shows no signs of abating in the short run. Longer term, the revelations by former National Security Agency contractor Edward Snowden about NSA tactics that allegedly include tapping the cellphones of as many as 35 world leaders threaten to undermine U.S. foreign policy in a range of areas. In Washington, demonstrators held up signs reading "Thank you, Edward Snowden!" as they marched and rallied near the U.S. Capitol to demand that Congress investigate the NSA's mass surveillance programs This vacuum-cleaner approach to data collection has rattled allies. "The magnitude of the eavesdropping is what shocked us," former French Foreign Minister Bernard Kouchner said in a radio interview. "Let's be honest, we eavesdrop too. Everyone is listening to everyone else. But we don't have the same means as the United States, which makes us jealous."

## Privacy and an Additional Controversy – Searches & the 4th Amendment (Area 3)

Even before the controversy related to mass surveillance (and also independent of it), there has always been debate related to what practices are fair for the police to engage in when searching for evidence of a crime. This debate centers around the Fourth Amendment, which protects individuals from unreasonable searches & seizures without probable cause of a crime being committed and police obtaining a warrant.

The [Fourth Amendment to the United States Constitution](http://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution) provides that:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[1]

Questions arise as to what constitutes “search.”

In the [United States v. Jacobson](mailto:http://supreme.justia.com/cases/federal/us/466/109/case.html%23113), the Supreme Court established that, “A *search* occurs when an expectation of privacy that society is prepared to consider reasonable is infringed.” In *Coolidge v. New Hampshire*, 403 U.S. 443 (1971), the Supreme Court said that a [search implies an invasion into private or hidden areas, including the body](mailto:http://www.kscoplaw.com/outlines/ssoutline.htm).

Warrants are generally required to conduct searches, but there are exceptions to this rule. A couple of examples --

First, individuals can consent to searches.

Second, when individuals do not have a reasonable expectation of privacy. For example, the Supreme Court has ruled that individuals do not have a reasonable expectation of privacy of the identifying information that is listed on the outside of an enveloped, even though they have an expectation of privacy related to the contents of the envelope.

Of course, there are many disputes related to what “reasonable” expectations of privacy that individuals may have that have led to a number of Supreme Court cases. In many of these cases, the Court said that individuals do not have a reasonable expectation of privacy.

* Governmental intrusion on an undeveloped area outside of the curtilage of a dwelling does not violate the reasonable expectation of privacy of the landowner. *Oliver v. United States*, 466 U.S. 170 (1984)

-  The Supreme Court held that warrantless aerial observation from an airplane lawfully in navigable airspace of a fenced-in backyard does not constitute a search within the meaning of the Fourth Amendment. *California v. Ciraolo*, 476 U.S. 463 (1986).

  - Police obtaining trash from bag deposited near the curb for collection is not a “search.” *California v. Greenwood*, 486 U.S. 35 (1988).

- By a trained dog of a suitcase to check for narcotics is not a "search" within the meaning of the Fourth Amendment. *United States v. Place*, 462 U.S. 696 (1983).

  --- Devices which monitor the telephone numbers called by an individual do not constitute searches under the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735 (1979).

-- Are not protected against governmental seizure because there is no legitimate expectation of privacy concerning the information kept in bank records. *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976).

    -- If an officer is in a place where he has the right to be and sees an item in plain view, he may search or seize the item so long as he has probable cause that the item is connected to criminal activity. *Harris v. United States*, 390 U.S. 234, 771-2 (1983).

- Police may make a limited exception to the probable cause and warrant requirements of the Fourth Amendment in that an officer may stop an individual if the officer has a reasonable and articulable suspicion, based on an objective view of facts previously known to him, or made known to him through observation, that the person stopped is committing, has committed, or is about to commit a crime. *Terry v Ohio*, 392 U.S. 1

More exceptions can be found [here](mailto:http://www.kscoplaw.com/outlines/ssoutline.htm) (where this list was drawn from).

It is important to note that the Fourth Amendment (and all Amendments) establish individual rights protects against *government* intrusions, not protections against private actions. So it is important to note that

## The Negative

### Answering the Privacy Advantage

First, Pro teams should minimizes the extent of the surveillance.  The NSA contends that it actually sees substantially [less than 1% of all internet traffic on a daily basis.](http://www.dailymail.co.uk/news/article-2390604/NSA-claims-reviews-00004-percent-Internet-traffic-daily-basis.html)

The NSA has claimed in a publicly-released document that it only reviews .00004% of Internet traffic on a daily basis.  The [**seven-page document**](http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf), titled ‘The National Security Agency: Missions, Authorities, Oversight and Partnerships,’ was released late Friday. It compares the amount of Internet data that the NSA collects to the size of a dime on a basketball court. ‘According to figures published by a major tech provider, the Internet carries 1,826 Petabytes of information per day. In its foreign intelligence mission, NSA touches about 1.6% of that,’ the agency states. ‘However, of the 1.6% of the data, only 0.025% is actually selected for review. The net effect is that NSA analysts look at 0.00004% of the world’s traffic in conducting their mission – that’s less than one part in a million.  Put another way, if a standard basketball court represented the global communications environment, NSA’s total collection would be represented by an area smaller than a dime on that basketball court.

Second, Pro teams should argue that the surveillance is subject to many safeguards and frequently reviewed. Although the US can collect the metadata, [it cannot indiscriminately sift through it.](http://www.csmonitor.com/USA/Justice/2013/0722/How-will-Obama-defend-secret-NSA-program-in-court-Letter-offers-clue)  If the government wants to take a closer look, it must any data gleaned must be associated with people or phone numbers already identified and approved by the secret Foreign Intelligence Surveillance Court. In 2012, the letter revealed, the court approved fewer than 300 “query terms” that would allow intelligence analysts to pursue a phone call further.   The protocols are overseen by the Justice Department and by intelligence officials.

The Pro should also work to de-prioritize the significance of the rights claim.

First, constitutional rights are not trump cards and can always be limited if there is a compelling government interest in doing so, such as the prevention of terrorism.

Amitai Etzioni, George Washington University Government Professor, THE SPIRIT OF COMMUNITY, 1993, p.26-7

When Communitarians argue that the pendulum has swung too far toward the radical individualistic pole and it is time to hurry its return, we do not seek to push it to the opposite extreme, of encouraging a community that suppresses individuality. We aim for a judicious mix of self-interest, self-expression, and commitment to the commons–of rights and responsibilities, of I and we. Hence the sociological recommendation to move from ‘I’ to ‘we’ is but a form of shorthand for arguing that a strong commitment to the commons must now be added to strong commitments to individual needs and interests that are already well ensconced. Balancing the domestic forces with a fair measure of resumed wellness will bring our society closer to a balanced position, without a significant tilt toward either side, a society able to steer a stable course.

Historically, Presidents have had a lot of discretion in limiting rights to protect national security.

Robert Pushaw, law professor, Pepperdine, 2011, National Security, Civil Liberties, and the War on Terror, ed. Katherine Darmer and Richard Fybel, p. 79-80

Initially, it is impossible to say with any certainty whether or not Presidents like Abraham Lincoln and Franklin Roosevelt had to infringe constitutional liberties the way they did in order to win their wars. Perhaps they could have achieved the same results with fewer intrusions. But maybe greater solicitude for personal freedoms would have led to defeat, or to a victory that exacted a far greater cost in blood and money. Speculating about such matters is an academic exercise. All we know for sure is that these Presidents took the actions they deemed necessary prevail, and they did. For better or worse, the Constitution commits to the President almost unbridled discretion to determine what must be done to meet a military emergency. These decisions must be made quickly and with imperfect information, and they are then judged by Congress, voters, and posterity

This is particularly true of privacy rights.

Silas Wasterstrom, law professor, GEORGETOWN LAW JOURNAL, October 1998, pp. 61-2

Unfortunately, however, a rights-based approach does not mesh very well with the structure of the fourth amendment. The amendment, as commonly understood, does not provide an absolute shield against even the most extreme invasions of privacy and liberty. It does not establish a right to privacy that trumps competing policy concerns. Instead, the fourth amendment prohibits searches only when the likelihood that the invasion will be productive fails to justify the cost. In its most general form, this translates into an insistence that the search be reasonable. When the Court attempts to give the requirement a somewhat more determinate content, it insists that the search be supported by “probable cause” or “reasonable suspicion.” In either case, however, the amendment requires no more than that the invasion be cost-justified in some sense.

Second, Americans experience limitations on privacy rights every day, including being subject to surveillance on street corners and shopping malls. We also freely give information to all of providers of web services that we use.

The Surveillance Society. By: Von Drehle, David, Calabresin, Massimo, Time International (South Pacific Edition), 8/12/2013, http://nation.time.com/2013/08/01/the-surveillance-society/

But the revelation of the **NSA’s vast data-collection programs** by a crusading contract worker, Edward Snowden, **has made it clear that the rise of technology is shattering even the illusion of privacy.** Almost overnight, and with too little reflection, t**he U.S. and other developed nations have stacked the deck in favor of the watchers. A surveillance society is taking root**. **Video cameras peer constantly from lamp poles and storefronts. Satellites and drones float hawkeyed through the skies. Smartphones relay a dizzying barrage of information about their owners to sentinel towers dotting cities and punctuating pastureland. License-plate cameras and fast-pass lanes track the movements of cars, which are themselves keeping a detailed record of their speed and location**. Meanwhile, **on the information superhighway, every stop by every traveler is noted and stored by Internet service providers like Google, Verizon and Comcast. Retailers scan, remember and analyze each purchase by every consumer**.

People divulge more “personal” information on websites like Facebook than the government would ever care to know about them.

Third, rights should not be viewed as absolute because if we did there would be no way of resolving conflicts between rights. In this specific context, there is arguably a right to security and [without security there cannot be liberty](http://www.heritage.org/Research/HomelandDefense/lm13.cfm). Fourth, debaters can engage in a strong defense of utilitarianism to argue that the greatest good for the greatest number is what should be protected. For a spirited discussion of the importance of not sacrificing society’s interests in the name of rights, you should consult Amitai Etzioni’s The Spirit of Community. Rights are not trump cards that should be used to sacrifice the collective to an individuals’ personal preferences and needs.   Rights must be balanced against the need for security, and in the era of a heightened risk of terrorism, and the large consequences that could result from another terror attack, it is important to balance the individual’s need for freedom against society’s need for security

Fourth, you should also argue that the resolution refers to the current surveillance measures and that if there is another significant terror attack that the security measures that will be adopted will be much more invasive than the ones that exist now.  If the terrorists attack again, there will be a much greater loss of personal freedom.

Americans are generally very concerned about the risk of another terror attack (rightly or wrongly), so arguments about the risks of terrorism will appeal to your judges.

### Disadvantages

There are a number of disadvantages. Some are particular to specific areas of privacy. Others are specific to particular areas.

*Politics (consumer, surveillance, crime).* There is political opposition to increasing the protection of privacy in all of these areas.

Consumer –

Surveillance

Crime –

*Terrorism (surveillance, crime)*. The primary objection to restricting government surveillance is that surveillance is [necessary to prevent terrorism](http://www.heritage.org/Research/HomelandDefense/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=69895) (and the largest, “nuclear terrorist attack” impacts are often referenced).

There are people who say a strong intelligence capability (that is enhanced through mass surveillance) is also necessary to prevent nuclear proliferation (the spread of nuclear weapons), position military forces, and conduct effective negotiations.

**Report and Recommendations of the President’s Review Group on Intelligence**, December 20**13**, Liberty and Security in a Changing World, December 12, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12\_rg\_final\_report.pdf

The national security threats facing the United States and our allies are numerous and significant, and they will remain so well into the future. These threats include international terrorism, the proliferation of weapons of mass destruction, and cyber espionage and warfare. A robust foreign intelligence collection capability is essential if we are to protect ourselves against such threats. Because our adversaries operate through the use of complex communications technologies, the National Security Agency, with its impressive capabilities and talented officers, is indispensable to keeping our country and our allies safe and secure.

But most of the focus is on the prevention of terrorism.

Given that, it is reasonable to ask, how many terrorists attacks have been prevented by NSA surveillance. Two specific examples are often cited.  One, surveillance advocates site use of phone meta data to identify an “operative” in San Diego who was providing financial assistance to terrorists in Somalia.   The second example is one involving a disrupted plot to bomb the New York City subway system. In the subway case, authorities used NSA’s Internet monitoring program to identify overseas communications involving Najibullah Zazi in Colorado. Zazi was later convicted in connection with the subway attack plan.

One thing is for certain is that there hasn’t been a significant terrorist attack in the US since 9/11.  Advocates of surveillance attribute the success in preventing these attacks to surveillance.  The [Arizona Republic editorializes](http://www.lasvegassun.com/news/2013/aug/21/when-nsa-oversteps-its-authority/) that “The government has a good record of preventing attacks, and these programs may be one big reason.”

Negative teams should really work to emphasize the risks and dangers of terrorism. For example, this quote highlights the risk:

**The U.S. State Department** **has renewed its global terrorism alert**, following the attack in Nairobi, Kenya, by a group claiming to be part of the Somalia-based al-Shabab.¶ Because of the “continuing threat of terrorist actions and violence” toward Americans, , U.S. citizens should “maintain a high level of vigilance.”¶ The department adds:¶ “**Current information suggests that al-Qaida, its affiliated organizations, and other terrorist groups continue to plan terrorist attacks against U.S. interests in multiple regions, including Europe, Asia, Africa, and the Middle East.** These attacks may employ a wide variety of tactics including suicide operations, assassinations, kidnappings, hijackings, and bombings.”¶ This caution replaces the one issued in February, but remember the State Department issued a rare worldwide-travel alert in August.¶ , the alert followed the Department State’s decision to close all its embassies and consulates across the Muslim world that weekend.¶ **Today’s caution says terrorists could target “high-profile sporting events, residential areas, business offices, hotels, clubs, restaurants, places of worship, schools, public areas, shopping malls, and other tourist destinations both in the United States and abroad where U.S. citizens gather in large numbers**, including during holidays.”[NPR](http://www.npr.org/blogs/thetwo-way/2013/09/25/226199162/state-department-renews-global-terror-alert)

[Other sources](http://www.lawfareblog.com/wp-content/uploads/2013/07/Strategic-Terrorism-Myhrvold-7-3-2013.pdf) highlight the danger:

The novelty of our present situation is that **modern technology can provide small groups of people with much greater lethality than ever before.** We now have to worry that private parties might gain access to weapons that are as destructive as—or possibly even more destructive than—those held by any nation-state. **A handful of people, perhaps even a single individual, now have the ability to kill millions or even billions**. Indeed, **it is perfectly feasible, from a technological standpoint, to kill every man, woman, and child on earth.**The gravity of the situation is so extreme that getting the concept across without seeming silly or alarmist is challenging. Just thinking about the subject with any degree of seriousness numbs the mind.¶ Worries about the future of the human race are hardly novel. Indeed, **the notion that terrorists or others might use weapons of mass destruction is so commonplace as to be almost passé.** spy novels, movies, and television dramas explore this plot frequently. **We have become desensitized** to this entire genre, in part because James Bond always manages to save the world in the end.

Negative teams need to emphasize that times have changed.  Not only was September 11th was the first time the US suffered a significant attack on its soil. In this case, it was a group being given protection by a foreign government.

Not only was this an attack on US soil for the first time, but it was also from a non-traditional actor (a terrorist group as opposed to a country), and the US began to realize that new technologies (the internet, message boards, cell phones) made it easier for potential terrorists to communicate and carry out attacks.   Advancing technology also makes it easier for terrorists to kill large numbers of people in single attacks, even absent potential attacks with nuclear, biological, or chemical weapons.   The new attacks, changing communications technologies, and the possibility of more advanced weapons meant that the government had to step-up its game in order to reduce the risk of another terror attack. The post-9/11 surveillance measures are designed to take these changes into account.

Affirmative essays will argue that terrorism can be prevented with targeted surveillance (assuming they don’t restrict that if the “crime” area is part of the resolution), but a strong argument can be made that targeted surveillance is not as effective as mass surveillance.

First, how would NSA know who a “foreign” terrorist was communicating with inside the United States unless they could also access domestic meta data? The US would have to target not only the foreign target but also the domestic suspect.

Second, if the metadata is collected then the government can instantly search the meta data it has if it is suspicious to find a tie between the potential terrorist and others.

Third, since any potential terrorist will communicate with people who the US doesn’t have a warrant for, collecting meta data is an inherent part of even targeted monitoring.

[Donald Scarinci](http://www.scarincihollenbeck.com/attorneys/partners/donald-scarinci/) is a New Jersey lawyer and managing partner of Scarinci Hollenbeck, LLC a regional law firm with offices in New York, New Jersey and Washington, D.C., April 24, 2014, http://blog.nj.com/njv\_donald\_scarinci/2014/04/is\_the\_nsa\_reading\_your\_emails.html

**While the NSA’s surveillance efforts are claimed to be targeted at foreigners, a rule change allows NSA analysts to discover and search U.S. citizens’ email, phone calls and databases without a warrant. As long as there is a reasonable belief the communications are foreign and overseas, content and metadata can be collected. The data is being collected under Section 702 of the of the Fisa Amendments Act** (FAA), which gives the NSA authority to target without warrant the communications of foreign targets, who must be non-US citizens and outside the US at the point of collection. However, “**incidental collection” also occurs**. This is the term used to refer to the purely domestic communications that can be inadvertently included in the surveillance sweeps.

[If the US had to stop “non-citizen” surveillance that inherently catches people in this process](http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html), it’s not clear how it could continue to function.

The collection depends on secret arrangements with foreign telecommunications companies or allied intelligence services in control of facilities that direct traffic along the Internet’s main data routes. Although the collection takes place overseas, two senior U.S. intelligence officials acknowledged that it sweeps in the contacts of many Americans. They declined to offer an estimate but did not dispute that the number is likely to be in the millions or tens of millions. A spokesman for the [Office of the Director of National Intelligence](http://www.dni.gov/index.php), which oversees the NSA, said the agency “is focused on discovering and developing intelligence about valid foreign intelligence targets like terrorists, human traffickers and drug smugglers. We are not interested in personal information about ordinary Americans.” The spokesman, Shawn Turner, added that rules approved by the attorney general require the NSA to “minimize the acquisition, use and dissemination” of information that identifies a U.S. citizen or permanent resident.

There is recent evidence that the [establishment of the Islamic Caliphant in Syria and Iraq will increase the risk of terroris](http://www.christianpost.com/news/isis-terror-group-declares-caliphate-in-iraq-syria-nails-9-men-to-cross-for-rebellion-122474/)m.

*Crime* (surveillance, crime). The link to crime is the same as it is to terrorism for the surveillance area – less surveillance makes it harder to stop crime. There are also links specific to the crime area, including dialing back searching.

*Business Confidence/internet economy* (consumer protection). This disadvantage only applies to the consumer privacy protection part of the topic.

*Presidential war powers*. Judicial and legislative restrictions on surveillance many infringe on the President’s war power authority.

### Counterplans

*Self-regulation* (consumer).

[Business2Community](mailto:http://www.business2community.com/big-data/gain-consumer-confidence-respecting-privacy-big-data-marketing-0930008%23By2UWRCWXyHFXWcI.99), July 4

Here are some of the viable strategies that can help marketers restore the ecosystem of trust between their business and the consumers.  
Read more at

* Before collecting the data of your consumers, make sure to take the time to evaluate what’s important data to ask the consumer to share that are only relevant for the big data analytics purpose.
* Provide a disclosure term to the consumers, making them understand how their is collected and used and for what purpose.
* Give the consumer the option to change their minds about consenting in tracking down their shopping activities. Giving them an opt out option will put them at ease knowing that they are not perpetually tied down and still in control of their privacy of whether to share their personal information or not.
* Create a trust framework between your business data collection policy and that of your customers. Give the consumers a detailed information about the tools you are using for gathering their personal data and the security process used in collecting them. Providing them the legal structure of your big data framework will also put them at ease.
* Use data by reference strategy where you can collect customer data by subscribing directly to your customer’s cloud data. This is very useful for bigger companies that collect huge repeated data from their customers. It is also a feasible cost effective solution for the rising data storage costs for companies. This will speed up the data sharing process between the digital marketing company and their client while giving the clients more control on what type of data and information will be available for data cloud sharing.
* Employ IT employees with a wider knowledge about data security and privacy, including the risks and available solutions in protecting their customers’ data and privacy.

*Executive order*. (Surveillance, some consumer, possibly police search).

*States.* Especially in the area of crime, the states could act to implement many of the reforms.

### Kritiks

There is always plenty of kritik ground on most topics, and many of the generic kritiks always apply, but there are a couple specific privacy kritiks.

*Feminism*. There are a number of authors who challenge protecting privacy on the grounds that it supports spousal abuse – the privacy makes it easier for men to abuse women in the home.

*Occularcentrism*. This kritik says it is bad to focus on visual privacy.

## Specific Plans – Surveillance

### 46 recommendations

In December 2013, the President’s Review Group on Intelligence and Communications Technologies suggested 46 different reforms that are detailed [here](mailto:http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf) –

[Summary here](mailto:http://justsecurity.org/4903/highlights-prgict/):

[Editor’s Note: *Just Security* is holding a “mini forum” on the [Report](http://justsecurity.org/wp-content/uploads/2013/12/2013-12-12_rg_final_report.pdf" \t "_blank)by the President’s Review Group on Intelligence and Communications Technologies. Others in the series include a post by Julian Sanchez examining the [scope of the NSA's section 702 program](http://justsecurity.org/2013/12/24/limited-702/), a post by David Cole and Marty Lederman analyzing [how metadata is used](http://justsecurity.org/2013/12/23/review-group-intelligence-communications-technologies-bulk-data-collection-section-215/) under section 215, a post by Jennifer Granick discussing the [implications for non-US persons](http://justsecurity.org/2013/12/18/presidents-review-board-says-protect-thy-neighbors-privacy/) (with a [follow-up post](http://justsecurity.org/2013/12/19/foreigners-review-group-report-part-2/) by Jennifer), and a post by Ryan Goodman discussing the [effectiveness of the section 215 metadata program](http://justsecurity.org/2013/12/27/effectiveness-telephony-metadata-program/).]

The [Report](http://justsecurity.org/wp-content/uploads/2013/12/2013-12-12_rg_final_report.pdf) of the President’s Review Group on Intelligence and Communications Technologies (PRGICT) has made quite a splash.  But what, exactly, is in it?  Tons of stuff, actually, on a huge range of subjects.  And 46 specific recommendations.

This post is a modest excavation of the Report, describing and clarifying what I see as its more interesting and important discussions and recommendations.  I will largely leave to others the task of assessing the merits of the Report’s various proposals.

This post is far from comprehensive; I do not, for instance, discuss the vast majority of the Report’s recommendations.  In particular, this post does not address one of the most important and controversial aspects of the Report–namely, its discussion of, and recommendations for, the Section 215 “telephony metadata” program and other bulk data collection programs.  The Report’s important discussion of the risks associated with data-mining of vast collections of information has not received the attention it deserves, having been overshadowed by the Report’s recommendation that such databases be maintained by third-party custodians rather than by the NSA.  David Cole and I will discuss these issues further in a [separate post](http://justsecurity.org/2013/12/23/review-group-intelligence-communications-technologies-bulk-data-collection-section-215/).

Here, I’ll start with some of the Report’s broader themes and general suggestions, and then proceed to some of the particulars.

**1.  WIDENING THE FOCUS**

It is commonly assumed that policy choices about the matters covered in the Report require a balancing between national security, on the one hand, and privacy, on the other.  As Jack Goldsmith [rightly emphasizes](http://www.lawfareblog.com/2013/12/40000-foot-reactions-to-presidents-review-group-report-and-recommendations/), however, the single most important characteristic of the Report is its insistence that much more is at stake than this binary opposition.

The Report repeatedly insists that, in deciding how to craft our surveillance practices, we must take account of not only the expected national security benefits and any intrusions on privacy when the government obtains information about individuals, but also other vital interests and likely effects—for example, the impact on social practices, and norms of communication and creativity, if the public comes to believe that its government has “total information awareness” capabilities; the potential effect of the practices on the U.S.’s reputation and diplomatic interests abroad—including prospects for U.S. initiatives to establish multilateral norms; and the possible impact on U.S. firms, and the U.S. economy.  Moreover, one of the important lessons of the Snowden revelations is that in assessing these various interests, policy makers should assume not that U.S. surveillance practices will remain secret, but instead that, for better or for worse, they may one day be publicized for all the world to see.  Would the benefits be worth the costs, along all of these metrics and more, if the program were to be exposed?  Much of the Report is written with that question in mind.

**2.  ESTABLISHING “FOUNDATIONS” THAT MIGHT WITHSTAND THE RISK OF OVERREACTION AFTER THE NEXT ATTACK**

A central premise of the Report is that many of the decisions the government made in the wake of 9/11 were precipitous and unbalanced, if understandable, and that it is therefore imperative to establish “secure foundations for future decisions” now, when decision-makers can assess various interests clearly and are not driven to “overreaction” in light of the inevitable fear and panic that follow catastrophic events (pp. 54, 57).  This passage on page 180 is representative:

[I]f a similar or worse incident or series of attacks were to occur in the future, many Americans, in the fear and heat of the moment, might support new restrictions on civil liberties and privacy.  The powerful existing and potential capabilities of our intelligence and law enforcement agencies might be unleashed without adequate controls.  Once unleashed, it could be difficult to roll back these sacrifices of freedom.

Our recommendations about NSA are designed in part to create checks and balances that would make it more difficult in the future to impose excessive government surveillance.  Of course, no structural reforms create perfect safeguards.  But it is possible to make restraint more likely.  Vigilance is required in every age to maintain liberty.

**3.  DISTINGUISHING BETWEEN SURVEILLANCE POLICIES FOR COMBAT AND NON-COMBAT OBJECTIVES**

Much has been made of Report’s recommendation (No. 22(3)) that the President should seriously consider appointing a civilian NSA Director.  But few have focused upon one of the principal reasons offered for that suggestion—namely, a concern that decisions about the scope of surveillance for *counterterrorism purposes generally* have been driven by the particular needs of the military for combat operations on the battlefields of Iraq and Afghanistan, thereby resulting in an “increasing overlap between signals intelligence for military purposes and the communications of ordinary Americans and citizens of other countries” (p. 186).  The authors suggest that perhaps surveillance policies and practices should be materially different in the two distinct settings (pp. 186-87):

The convergence of military and civilian communications is important in light of the drastically different expectations of government surveillance.  In wartime, during active military operations, signals intelligence directed at the enemy must be highly aggressive and largely unrestrained. . . .  [T]here are powerful arguments for strong measures to intercept communications to prevent or detect attacks on American troops in Iraq and Afghanistan.  During military operations, the goal is information dominance, to protect the lives and safety of US forces and to meet military objectives.  The same rules do not apply on the home front.

A significant challenge today is that a wide and increasing range of communications technologies is used in both military and civilian settings.  The same mobile phones, laptops, and other consumer goods used in combat zones are often used in the rest of the world.  The same is true for software, such as operating systems, encryption protocols, and applications.  Similarly, routers, fiber optic, and other networking features link combat zones with the rest of the global Internet.  Today, no battlefield lines or Iron Curtain separates the communications in combat zones from the rest of the world.   A vulnerability that can be exploited on the battlefield can also be exploited elsewhere.  The policy challenge is how to achieve our military goals in combat zones without undermining the privacy and security of our communications elsewhere.  In responding to this challenge, it remains vital to allow vigorous pursuit of military goals in combat zones and to avoid creating a chilling effect on the actions of our armed forces there.

The public debate has generally focused on the counterterrorism rationale for expanded surveillance since the terrorist attacks of September 11, 2001.  **We believe that the military missions in Iraq and Afghanistan have also had a large but difficult-to-measure impact on decisions about technical collection and communications technologies.**  **Going forward, even where a military rationale exists for information collection and use, there increasingly will be countervailing reasons not to see the issue in purely military terms**.  The convergence of military and civilian communications supports our recommendations for greater civilian control of NSA as well as a separation of NSA from US Cyber Command.  **It is vital for our intelligence agencies to support our warfighters, but we must develop governance structures attuned to the multiple goals of US policy**.

The Report does not provide further details with respect to this suggestion; but it does offer food for thought about whether Congress and the Executive ought to consider developing a kind of “two-track” surveillance regime, in which the rules respecting surveillance in support of combat missions might be more robust, and subject to different checks, than the rules that govern national security surveillance for other objectives.  In this respect, the Report is reminiscent of the President’s [May 23d National Defense University speech](http://justsecurity.org/2013/10/15/23d-ndu-speech-action-broader-significance-al-liby-ikrima-operations/), in which he suggested that perhaps the rules for use of force ought to be different “outside the Afghan theater,” where force protection is less of a concern.  (See [my post with Mary DeRosa](http://justsecurity.org/2013/10/15/23d-ndu-speech-action-broader-significance-al-liby-ikrima-operations/) for more along these lines.)

**4.  TRANSPARENCY AND WHISTLE-BLOWING**

a.  Transparency.  One of the most important questions in the wake of the Snowden leaks is whether it was a mistake for the government to keep secret the existence of programs such as the telephony metadata bulk collection program; the general scope of other programs that are nominally acknowledged (such as FAA Section 702 surveillance); and the “minimization” rules that cabin such programs.  Should the robust public debate we’re having now have occurred *before* these programs were initiated?  Should the documents now prominently displayed on the ODNI website have been kept secret all these years?  Or, more to the point, under what circumstances, and to what degree, should proposed *future* programs be publicly debated before they are authorized?

The Report’s authors conclude that “[t]here is a compelling need today for a serious and comprehensive reexamination of the balance between secrecy and transparency” (p.125); but they also recognize that the “most vexing problems” in this regard “arise when the public disclosure of secret information is *both* harmful to national security and valuable to informed self-governance” (p.125).

Their principal recommendation on this question, Recommendation No. 7, is somewhat indeterminate:

[L]egislation should be enacted requiring that **detailed information** about authorities such as those involving National Security Letters, section 215 business records, section 702, pen register and trap-and-trace, and the section 215 bulk telephony meta-data program should be made available on a regular basis to Congress and the American people to the greatest extent possible, **consistent with the need to protect classified information**. With respect to authorities and programs whose existence is unclassified, there should be a strong presumption of transparency to enable the American people and their elected representatives independently to assess the merits of the programs for themselves.

This begs the question somewhat, since the real difficulty is deciding when the information ought to be classified in the first instance.  More important, then, is Recommendation No. 11, which suggests a strengthening of procedural and substantive standards for secrecy/classification decisions:

We recommend that the decision to keep secret from the American people programs of the magnitude of the section 215 bulk telephony meta-data program should be made **only after careful deliberation at high levels of government and only with due consideration of and respect for the strong presumption of transparency that is central to democratic governance**.  A program of this magnitude should be kept secret from the American people only if (a) the program serves a compelling governmental interest and (b) the efficacy of the program would be ***substantially***impaired if our enemies were to know of its existence.  (Italics in original.)

b.  Whistle-blowing and the CLPP Board.  The Report also includes one intriguing recommendation (No. 27(2)) with respect to whistle-blowers—enactment of a statute that would give employees within the Intelligence Community who are concerned about secret programs the authority to “report their concerns directly” to a “newly chartered, strengthened, independent Civil Liberties and Privacy Protection Board.”

The Report does not describe the ways in which the CLPP Board would be “independent” from the President, nor what it would be empowered to do with the information it receives from such whistle-blowers—details that would need to be worked out in order for the Executive and Congress to fairly evaluate this recommendation.

**5.  ENCRYPTION**

Not surprisingly, Recommendation No. 29(2) has received a great deal of attention.  It provides that the U.S. should not “in any way subvert, undermine, weaken, or make vulnerable generally available commercial software.”  The Report further urges the government to “make it clear” that “NSA will not engineer vulnerabilities into the encryption algorithms that guard global commerce,” nor “demand changes in any product by any vendor for the purpose of undermining the security or integrity of the product, or to ease NSA’s clandestine collection of information by users of the product” (p. 218).

The Report itself suggests, without elaboration, that these proposals would not deviate substantially from the status quo, since “it appears that in the vast majority of generally used, commercially available encryption software, there is no vulnerability, or ‘backdoor,’ that makes it possible for the US Government or anyone else to achieve unauthorized access” (p.217).

I’ll leave it to others to discuss in greater detail whether and to what extent these recommendations would alter current practices, and whether they would be too restrictive or not restrictive enough.  I would simply note that the authors were very careful here to use terms and qualifications that avoid categorical assertions (“generally available,” “commercial,” “demand,” “appears,” “vast majority,” “generally used,” etc.).  The Report might fairly be read, therefore, to leave plenty of play in the joints concerning how and to what extent adoption of Recommendation 29(2) would require changes in current practices.

**6.  SURVEILLANCE OF FOREIGN PERSONS OVERSEAS**

This part of the Report has been subject to some unwarranted caricature.  As far as I can tell, for instance, the Report does not, as Joel Brenner [alleges](http://www.lawfareblog.com/2013/12/a-fruitcake-of-a-report/), “recommend[] that we treat foreigners and U.S. persons alike under the law.”

It does, however, make one recommendation that would, I believe, have fairly significant ramifications.

At page 172, the Report explains that national security is hardly the only reason that the U.S. (or any other nation) engages in foreign espionage:

In [some] instances, information might be sought in order to learn about the intentions of the leaders of other nations, even when no threat to our national security is involved.  The latter instances might involve an interest in acquiring information that might prove useful as United States officials plan for meetings and discussions with other nations on bilateral economic issues.  In such circumstances, it might be helpful to know in advance about another nation’s internal concerns and priorities or about its planned negotiating strategy but it is not critical to national security.  Different interests have different weights.

Yet in Recommendation No. 13(2), the authors urge the government to “reaffirm” (?) that “in implementing section 702, **and any other authority that authorizes the surveillance of non-United States persons who are outside the United States**, . . . such surveillance “must be directed *exclusively* at the national security of the United States or our allies” (emphasis added).

This appears to suggest that the sorts of economic, political and diplomatic surveillance the authors later describe as part of current practice would be out of bounds.  I don’t know if that was their intent–perhaps, for example, this limit is not supposed to apply to surveillance of foreign officials and other public figures.  But to the extent Recommendation No. 13(2) were construed to have such an effect, it could be very significant, indeed.  It is unlikely the U.S. or any other nation would ever adopt any such “for national security purposes only” limitation.  Placing greater limits on such non-security-based surveillance?  Sure.  But an absolute prohibition?  Doubtful.

**7.  INCIDENTAL COLLECTION OF U.S. PERSON COMMUNICATIONS AND INFORMATION**

a.  Minimization.  Recommendation No. 12 is undoubtedly one of the most important and provocative in the Report.  It would impose new limits (or minimization rules) on what can be done with communications of, and information about, U.S. persons that are collected during anysurveillance of foreigners–under Section 702 of the FAA, Executive Order 12,333, or otherwise:

We recommend that, if the government legally intercepts a communication under section 702, **or under any other authority that justifies the interception of a communication on the ground that it is directed at a non-United States person who is located outside the United** **States**, and if the communication either includes a United States person as a participant or reveals information about a United States person:

(1) any information about that United States person should be purged upon detection unless it either has foreign intelligence value or is necessary to prevent serious harm to others;

(2) any information about the United States person may not be used in evidence in any proceeding against that United States person; [and]

(3) the government may not search the contents of communications acquired under section 702, or under any other authority covered by this recommendation, in an effort to identify communications of particular United States persons, except (a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism.

If I’m not mistaken, this would have at least two important effects.  First, subsection (3) would prohibit the “secondary” search (I believe others have referred to it as a “back-door” search) of collected, foreign-targeted communications for U.S. person communications, except in circumscribed situations.

More importantly, perhaps, if foreign-targeted surveillance incidentally reveals information about U.S. person *wrongdoing*, or criminal activity, that information could not be used as evidence against the U.S, person, and indeed would have to be “purged” from government records altogether, and not be the basis for further investigation, “unless it either has foreign intelligence value or is necessary to prevent serious harm to otherscommunications.”

I don’t know enough to be certain, but such limitations might be a significant change from current practices.

b.  Limits on Section 702 Surveillance?  The Report contains an interesting clue about how the government is presently using Section 702 that I do not recall being previously disclosed—and raises a related question about legal authorities under that provision of the FAA:

The Report explains (page 136) that in implementing Section 702, “NSA identifies specific ‘identifiers’ (for example, e-mail addresses or telephone numbers) that it reasonably believes are being used by non-United States persons located outside of the United States to communicate foreign intelligence information within the scope of the approved categories (e.g., international terrorism, nuclear proliferation, and hostile cyber activities).  NSA then acquires the content of telephone calls, e-mails, text messages, photographs, and other Internet traffic using those identifiers from service providers in the United States.”  A footnote adds that “[i]llustrative identifiers might be an e-mail account used by a suspected terrorist abroad or other means used by high-level terrorist leaders in two separate countries to pass messages. The number of identifiers for which NSA collects information under section 702 has gradually increased over time.”

Later, on pages 152-53, the authors “emphasiz[e] that, contrary to some representations, **section 702 does not authorize NSA to acquire the content of the communications of masses of ordinary people**.  To the contrary, section 702 authorizes NSA to intercept communications of non-United States persons who are outside the United States **only if it reasonably believes that a particular ‘identifier’ (for example, an e-mail address or a telephone number) is being used to communicate foreign intelligence information related to such matters as international terrorism, nuclear proliferation, or hostile cyber activities**.”  (Italics in original.)

I may be mistaken, but I don’t believe that there’s anything in the statute itself that imposes the limitations in bold–neither that the NSA must use such “identifiers,” nor that international terrorism, nuclear proliferation, and hostile cyber activities are the only topics of acceptable foreign intelligence information that can be sought.  Perhaps the FISC Court has insisted upon such limits; but, as far as I know, the Section 702 authority as currently codified is not so circumscribed.

**8.  NATIONAL SECURITY LETTERS**

As I read it, the Report in effect proposes (page 93 and note 83) the wholesale repeal of National Security Letter (NSL) authorities:

We are unable to identify a principled reason why NSLs should be issued by FBI officials when section 215 orders and orders for pen register and trap-and-trace surveillance must be issued by the FISC. . . .  NSLs should not issue without prior judicial approval, in the absence of an emergency where time is of the essence. . . .  It is essential that the standards and processes for issuance of NSLs match as closely as possible the standards and processes for issuance of section 215 orders. Otherwise, the FBI will naturally opt to use NSLs whenever possible in order to circumvent the more demanding – and perfectly appropriate – section 215 standards.

That would certainly be a significant change from current law.

### Repeal or modify Executive Order 12333

John Napier Tye, July 18, 2014 served as section chief for Internet freedom in the State Department’s Bureau of Democracy, Human Rights and Labor from January 2011 to April 2014. He is now a legal director of [Avaaz](http://www.avaaz.org/en/), a global advocacy organization, Washington Post, http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2\_story.html

From 2011 until April of this year, I worked on global Internet freedom policy as a civil servant at the State Department. In that capacity, I was cleared to receive top-secret and “sensitive compartmented” information. Based in part on classified facts that I am prohibited by law from publishing, I believe that Americans should be even more concerned about the collection and storage of their communications under Executive Order 12333 than under Section 215.

Bulk data collection that occurs inside the United States contains built-in protections for U.S. persons, defined as U.S. citizens, permanent residents and companies. Such collection must be authorized by statute and is subject to oversight from Congress and the Foreign Intelligence Surveillance Court. The statutes set a high bar for collecting the content of communications by U.S. persons. For example, Section 215 permits the bulk collection only of U.S. telephone metadata — lists of incoming and outgoing phone numbers — but not audio of the calls.

[Executive Order 12333](http://www.archives.gov/federal-register/codification/executive-order/12333.html) contains no such protections for U.S. persons if the collection occurs outside U.S. borders. Issued by President Ronald Reagan in 1981 to authorize foreign intelligence investigations, 12333 is not a statute and has never been subject to meaningful oversight from Congress or any court. Sen. Dianne Feinstein (D-Calif.), chairman of the Senate Select Committee on Intelligence, [has said](http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html) that the committee has not been able to “sufficiently” oversee activities conducted under 12333.

Unlike Section 215, the executive order authorizes collection of the content of communications, not just metadata, even for U.S. persons. Such persons cannot be individually targeted under 12333 without a court order. However, if the contents of a U.S. person’s communications are “incidentally” collected (an [NSA term of art](http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html)) in the course of a lawful overseas foreign intelligence investigation, then Section 2.3(c) of the executive order explicitly authorizes their retention. It does not require that the affected U.S. persons be suspected of wrongdoing and places no limits on the volume of communications by U.S. persons that may be collected and retained.

“Incidental” collection may sound insignificant, but it is a legal loophole that can be stretched very wide. Remember that the NSA is building a data center in Utah five times the size of the U.S. Capitol building, with its own power plant that will reportedly burn $40 million a year in electricity.

“Incidental collection” might need its own power plant.

A legal regime in which U.S. citizens’ data receives different levels of privacy and oversight, depending on whether it is collected inside or outside U.S. borders, may have made sense when most communications by U.S. persons stayed inside the United States. But today, U.S. communications increasingly travel across U.S. borders — or are stored beyond them. For example, the Google and Yahoo e-mail systems rely on networks of “mirror” servers located [throughout the world](http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html). An e-mail from New York to New Jersey is likely to wind up on servers in Brazil, Japan and Britain. The same is true for most purely domestic communications.

Executive Order 12333 contains nothing to prevent the NSA from collecting and storing all such communications — content as well as metadata — provided that such collection occurs outside the United States in the course of a lawful foreign intelligence investigation. No warrant or court approval is required, and such collection never need be reported to Congress. None of [the reforms that Obama announced](http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/17/everything-you-need-to-know-about-obamas-nsa-reforms-in-plain-english/) earlier this year will affect such collection.

Without any legal barriers to such collection, U.S. persons must increasingly rely on the affected companies to implement security measures to keep their communications private. The executive order does not require the NSA to notify or obtain consent of a company before collecting its users’ data.

The attorney general, rather than a court, must approve “minimization procedures” for handling the data of U.S. persons that is collected under 12333, to protect their rights. I do not know the details of those procedures. But the director of national intelligence recently [declassified a document](http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf) (United States Signals Intelligence Directive 18) showing that U.S. agencies may retain such data for five years.

Before I left the State Department, I filed a complaint with the department’s inspector general, arguing that the current system of collection and storage of communications by U.S. persons under Executive Order 12333 violates the Fourth Amendment, which prohibits unreasonable searches and seizures. I have also brought my complaint to the House and Senate intelligence committees and to the inspector general of the NSA.

I am not the first person with knowledge of classified activities to publicly voice concerns about the collection and retention of communications by U.S. persons under 12333. The president’s own Review Group on Intelligence and Communication Technologies, in Recommendation 12 of [its public report](http://apps.washingtonpost.com/g/page/world/nsa-review-boards-report/674/), addressed the matter. But the review group coded its references in a way that masked the true nature of the problem.

At first glance, Recommendation 12 appears to concern Section 702 of the FISA Amendments Act, which authorizes collection inside the United States against foreign targets outside the United States. Although the recommendation does not explicitly mention Executive Order 12333, it does refer to “any other authority.” A member of the review group confirmed to me that this reference was written deliberately to include Executive Order 12333.

Recommendation 12 urges that all data of U.S. persons incidentally collected under such authorities be immediately purged unless it has foreign intelligence value or is necessary to prevent serious harm. The review group further recommended that a U.S. person’s incidentally collected data never be used in criminal proceedings against that person, and that the government refrain from searching communications by U.S. persons unless it obtains a warrant or unless such searching is necessary to prevent serious harm.

The White House understood that Recommendation 12 was intended to apply to 12333. That understanding was conveyed to me verbally by several White House staffers, and was confirmed in an unclassified White House document that I saw during my federal employment and that is now in the possession of several congressional committees.

In that document, the White House stated that adoption of Recommendation 12 would require “significant changes” to current practice under Executive Order 12333 and indicated that it had no plans to make such changes.

All of this calls into question some recent administration statements. Gen. Keith Alexander, a former NSA director, has said publicly that for years the NSA maintained a U.S. person e-mail metadata program similar to the Section 215 telephone metadata program. And he has maintained that the e-mail program was terminated in 2011 because [“we thought we could better protect civil liberties and privacy by doing away with it.”](http://abcnews.go.com/blogs/politics/2013/06/nsa-chief-on-email-collection-nsa-deleted-data-wanted-to-protect-privacy/) Note, however, that Alexander never said that the NSA stopped collecting such data — merely that the agency was no longer using the Patriot Act to do so. I suggest that Americans dig deeper.

Consider the possibility that Section 215 collection does not represent the outer limits of collection on U.S. persons but rather is a mechanism to backfill that portion of U.S. person data that cannot be collected overseas under 12333.

Proposals for replacing Section 215 collection are currently being debated in Congress. We need a similar debate about Executive Order 12333. The order as used today threatens our democracy. There is no good reason that U.S. citizens should receive weaker privacy and oversight protections simply because their communications are collected outside, not inside, our borders.

I have never made any unauthorized disclosures of classified information, nor would I ever do so. I fully support keeping secret the targets, sources and methods of U.S. intelligence as crucial elements of national security. I was never a disgruntled federal employee; I loved my job at the State Department. I left voluntarily and on good terms to take a job outside of government. A draft of this article was reviewed and cleared by the State Department and the NSA to ensure that it contained no classified material.

When I started at the State Department, I took an oath to protect the Constitution of the United States. I don’t believe that there is any valid interpretation of the Fourth Amendment that could permit the government to collect and store a large portion of U.S. citizens’ online communications, without any court or congressional oversight, and without any suspicion of wrongdoing. Such a legal regime risks abuse in the long run, regardless of whether one trusts the individuals in office at a particular moment.

### Repeal or modify section 702

Eva Galperin and Nadia Kayyali, July 14, 2014, http://personalliberty.com/nsa-spying-now-personal/

Imagine that you watched a police officer in your neighborhood stop ten completely ordinary people every day just to take a look inside their vehicle or backpack. Now imagine that nine of those people are never even accused of a crime. They just happened to be in the wrong place at the wrong time. Even the most law-abiding person would eventually protest this treatment. In fact—[they have](http://changethenypd.org/issue).

Now replace police officers with the NSA. The scenario above is what the NSA is doing with our communications, under cover of its [twisted interpretation](https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why) of Section 702 of the FISA Amendments Act. *The Washington Post* has [revealed](http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html) that “Nine of 10 account holders found in a large cache of intercepted conversations, which former NSA contractor Edward Snowden provided in full to *The Post*, were not the intended surveillance targets.” Additionally, “[n]early half of the surveillance files, a strikingly high proportion, contained names, e-mail addresses or other details that the NSA marked as belonging to U.S. citizens or residents.”

The thousands of pages of documents that provide that basis for the article are not raw content. Rather, as Barton Gellman, one of the authors of the article states in a [follow up](http://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html) published several days later states: “Everything in the sample we analyzed had been evaluated by NSA analysts in Hawaii, pulled from the agency’s central repositories and minimized by hand after automated efforts to screen out U.S. identities.”

What that means is that if you’re on the Internet, you’re in the NSA’s neighborhood—whether you are in the U.S. or not. And like those who protest unjust policies like stop and frisk in their cities, you should be protesting this treatment.

This revelation is significant because it proves the point privacy and civil liberties advocates have been making for years: NSA surveillance is not narrowly targeted. EFF’s legal fight against the NSA’s warrantless mass surveillance program has been ongoing [since 2006](https://www.eff.org/nsa-spying/timeline), but *The Washington Post*’s statistics about 160,000 intercepts they have analyzed from the Snowden files indicate that even what the NSA calls “targeted” surveillance is far from narrow in scope.  In fact, it is so bloated that we should all be questioning its necessity and efficacy at this point. Taken hand in hand with [The Intercept’s article](https://firstlook.org/theintercept/article/2014/07/09/under-surveillance/) outlining the targeting of five civil rights and political leaders from the Muslim-American community, our outrage should be palpable.

What’s more, the report comes on the heels of a debate specifically about Section 702 that has been brewing in Congress for months, as civil liberties champions like Senator Ron Wyden and Representative Zoe Lofgren [question](http://www.wyden.senate.gov/news/press-releases/wyden-releases-details-of-backdoor-searches-of-americans-communications) and [work to address](http://lofgren.house.gov/news/documentsingle.aspx?DocumentID=385397) how the NSA uses this authority. This revelation should make it clear to the Senate when it considers the USA FREEDOM Act: Section 702 needs to be reformed. [Cosmetic changes](https://www.eff.org/deeplinks/2014/05/eff-dismayed-houses-gutted-usa-freedom-act) to NSA spying, or even substantive changes to Section 215 bulk telephone records collection, are insufficient. Unbridled, unconstitutional collection of the contents of communications needs to end.

*The Washington Post* article is based on a comprehensive review of thousands of pages of documents. In fact, as the article points out: “No government oversight body, including the Justice Department, the Foreign Intelligence Surveillance Court, intelligence committees in Congress or the president’s Privacy and Civil Liberties Oversight Board, has delved into a comparably large sample of what the NSA actually collects.” What’s more, these are documents that government officials have repeatedly insisted Edward Snowden would never have been able to access.

Regardless of the government’s denials, Snowden did have these documents, and now we know at least some of what they contained. So does Congress. So there’s no excuse anymore for the type of [maneuvering](http://lofgren.house.gov/news/documentsingle.aspx?DocumentID=380797) that led to the gutting of USA FREEDOM in the House.  More importantly, there’s no excuse for the Senate to ignore Section 702 when it considers USA FREEDOM.

Real NSA reform from Congress will, among other things, shut the backdoor that allows the NSA to access American’s communications. It will also end collection of communications “about” a target.

Of course, none of this solves the problem of how NSA surveillance affects non-U.S. persons. One of the shocking things about *The Washington Post*’s article is its description of the communications intercepted:

Scores of pictures show infants and toddlers in bathtubs, on swings, sprawled on their backs and kissed by their mothers. In some photos, men show off their physiques. In others, women model lingerie, leaning suggestively into a webcam or striking risque poses in shorts and bikini tops.

We are no longer talking about statistics. We are talking about real people going about their daily lives. It is not surprising to learn that in the course of its investigations, the NSA gathers up a considerable number of communications that prove to be insignificant, irrelevant, or (as is the case with communications between US persons) outside the scope of their work. What is shocking is that the NSA keeps this enormous trove of personal data about people it should not be watching in the first place. It appears that the unspoken coda to General Alexander’s “[collect it all](http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html)” motto is “and never throw it away.”

### FISA court reform – special advocate

[Time, July 14](mailto:http://time.com/2970766/privacy-freedom-act-reform-secret-nsa-oversight-fisa/)

Privacy advocates renewed their calls for reforms at the Foreign Intelligence Surveillance Court on Tuesday, after a new report revealed documents leaked by Edward Snowden that detail secret intelligence warrants against five American Muslims.

The targeted individuals, found on a list of thousands of mostly foreign targets for court-reviewed surveillance, include a professor at Rutgers University, a former Bush administration official and the executive director of the nation’s largest Muslim civil rights group. Because the Justice Dept. and the FBI refused to comment, it is unknown on what grounds the men were targeted for surveillance, nor is it clear under what precise legal authority the surveillance was conducted.

Civil libertarians say the report shows why the U.S. Congress should introducing a special advocate on the court, whose job it would be to represent civil liberties interests in court proceedings, and establishing a process for declassifying the court’s orders. Those reforms are included in a Senate version of an intelligence reform bill, but not the House version now under consideration.

“It’s been one of the core issues lacking in the debate,” said Mark Jaycox, a legislative analyst with the Electronic Frontier Foundation, about the process by which secret warrants can be obtained from the secret court. To get a FISA warrant, the NSA does have to explain to the court who it wants to spy on and why, as well as what they hope to get from the surveillance, but the bar is significantly lower than in a civilian courtroom. “I would call it a Probable Cause Warrant Light,” Jaycox said. “It’s not the high standard of a probably cause warrant.”

### General improvements and transparency

Danie Byman, Foreign Affairs, May 2014, http://www.foreignaffairs.com/articles/141215/daniel-byman-and-benjamin-wittes/reforming-the-nsa

To set a clearer agenda for reform, the NSA should begin by dividing its activities into three broad categories. First, the agency should identify what it really must keep secret. In truth, only a fraction of the NSA’s current activities -- penetrating new technologies, for example, or monitoring supposedly secret systems of U.S. rivals, such as China -- are so sensitive that the mere revelation of their existence would damage U.S. interests.

The NSA needs to work harder to keep those programs hidden by granting far fewer people access to them. Anderson said that stricter controls on access are already in the works, with a system to tag each piece of data that the NSA collects and each user. Data and user tags could then be matched depending on the user’s privileges. Keeping access to the most important secrets limited to a smaller circle of confidants would make it more likely that they stayed secret.

But a push for more secrecy will provoke new fears of future abuses. Keeping fewer people in the loop would also increase the risk that important dots could go unconnected. Anderson acknowledged this risk, saying the agency is currently erring on the side of data security at the expense of effectiveness. There is no way to resolve that dilemma: to preserve secrecy, the NSA will have to forgo the benefit of having lots of eyes on a problem. But this tradeoff is sometimes worthwhile, since it ensures that the most important programs are privy to only a select group of analysts.

When it comes to the agency’s less sensitive work that has not yet been exposed, the NSA should be prepared to abandon it if the benefits do not outweigh the costs of disclosure. Some spying on allies, for example, should be reconsidered, as Obama has already committed to doing. The practice in itself is not wrong, and it often yields valuable findings. But just as often, the benefits are not worth the price.

Third, the NSA must lift the veils over certain programs it means to continue. Because of Snowden’s leaks and subsequent disclosures and declassifications, the metadata collection program, for example, is not a secret -- and so even if some version of it continues, it makes sense to err on the side of openness going forward. More generally, the NSA should disclose more information to the public about the scope and scale of politically sensitive surveillance, where possible, and even more specifics to Congress. Bringing in civil liberties groups to discuss the parameters of some programs involving the surveillance of U.S. citizens would also help. The NSA is not likely to convince such groups to take the agency’s side, but it could still explain to them its procedures for minimizing intrusions.

Becoming more open will require a shift in the institutional culture of the NSA and in the intelligence community more generally. But that shift is already taking place. In 2012, the NSA’s then deputy director, John Inglis, quipped that the agency is “probably the biggest employer of introverts” in the federal government. But over the past few months, the country’s most powerful introverts have begun speaking out publicly to an unprecedented degree. Last December, senior NSA officials even agreed to participate in a lengthy series of podcasts with one of us on the future direction of the agency.

Ultimately, increasing the transparency of the NSA and boosting oversight of its activities will have serious operational consequences. Those changes may at times slow down surveillance or make the agency more hesitant to acquire data that, in hindsight, would have been useful for counterterrorism or other essential operations. But conducting intelligence in public, at least to a certain degree, will help preempt scandals and allow the NSA to educate policymakers and journalists about what it does and why.

Despite Snowden’s leaks, much of the public still misunderstands how the NSA works and what it does. In the past, the agency has welcomed this ignorance, since it helped the government keep its secrets secure. But now that the cat is out of the bag, the NSA, mindful of the value of public trust, needs to recalibrate its operations in order to increase public understanding of how it works. The necessary reforms will, to one degree or another, require Americans to take on more risk -- a decision that will lead to political criticism should another terrorist attack occur on U.S. soil. If done well, however, the reforms will also make the agency more sensitive to public concerns while preserving its necessary core capabilities.

### Amendments to USA Freedom Act

Center for Democracy & Technology, June 26, https://cdt.org/blog/key-changes-needed-to-the-usa-freedom-act-h-r-3361/

While there is likely no “silver bullet” to solving the bulk collection problem, making several further revisions to the USA FREEDOM Act can alleviate the risk of overbroad collection while providing government with the necessary flexibility to protect security:

1. *New Minimization Procedures*: Congress should add new minimization procedures to the bill that would limit – to the greatest degree possible – the acquisition, retention, and use of surveillance to targets of investigations, suspected agents of foreign powers, and direct contacts of such individuals.
2. *Clear Statement of Purpose*: The bill’s definition of “Specific Selection Term” should clearly state that its purpose is to narrowly tailor collection to affect as few extraneous individuals as possible.
3. *Negative Clause*: A non-exclusive negative clause should be added to the bill’s definition of Specific Selection Term,” clarifying it cannot be used to denote large geographic areas such as area codes, zip codes, cities, or states.

### Additional proposed reforms

Center for Democracy& Technology, June 26, https://cdt.org/blog/key-changes-needed-to-the-usa-freedom-act-h-r-3361/

Further Action is Needed on Other Important Issues

Prohibiting bulk collection is the most critical issue regarding the USA FREEDOM Act, and support of many privacy advocates and businesses will likely hinge on this issue.  However, other important reforms that the bill should address include the following:

1. *Section 702*: While more Americans are currently affected by the NSA’s ongoing bulk collection program, significant problems exist regarding the PRISM and Upstream programs conducted under Section 702 of FISA.  As CDT has [stated before](https://cdt.org/blog/cdt-proposes-collection-and-retention-limits-on-section-702-surveillance" \t "_blank), the serious issues with Sec. 702 infringe upon American’s Fourth Amendment rights, harm the human rights of individuals abroad, and are [drastically damaging](http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry" \t "_blank) the American tech industry globally.  The USA FREEDOM Act should remove its reference to “about” communications, which have never been authorized by statute, and close the backdoor search loophole, which permits the NSA to deliberately seek out Americans’ communications without court approval.  Further, Congress should commit to a comprehensive review of Section 702 in the future.
2. *Transparency*:  Sec. 604 of the USA FREEDOM Act provides valuable improvements to transparency by permitting new company reporting, however greater reporting can be allowed without compromising ongoing operations.  The bill should permit reporting on separate legal authorities in bands of 250, rather than require – as the bill currently does – that companies lump orders under all authorities together.  Further, the bill should enhance reporting accuracy by permitting reporting of “accounts affected” rather than “selectors targeted.”
3. *Special Advocate*:  Currently, Sec. 401 of the USA FREEDOM Act merely encourages amicus participation, with no statutory charge regarding what issues to advocate.  The bill should create a special Advocate, specifically tasked with vigorously defending privacy, civil liberties, and transparency in important FISC proceedings.  This would more effectively prevent unnecessarily broad surveillance, enhance the value of Court declassifications, and help restore public trust in the FISC.

### Additional (2) proposed reforms

IVN.US, July 7, 2014, http://ivn.us/2014/07/07/senators-want-restore-improve-transparency-usa-freedom-act/

Senators want to restore and improve transparency in the US Freedom Act

A bipartisan team of U.S. Senators is [hoping](http://techfreedom.org/post/90586268284/bipartisan-senate-duo-presses-obama-to-revitalize-usa" \t "_blank) legislation can eventually gain the support of President Barack Obama and curb some of the powers of the National Security Agency (NSA).

Originally sponsored by U.S. Senators Al Franken and Dean Heller as part of their Surveillance Transparency Act, these lawmakers believe the measures can benefit the USA Freedom Act. According to a press release, an [amended USA Freedom Act](https://www.franken.senate.gov/?p=press_release&id=2881" \t "_blank) would:

“Force the government to release the number of Americans who have had their information not only collected under these surveillance programs, but also reviewed. They would also give companies greater flexibility to tell their customers approximately how many of them were caught up in government surveillance requests.”

Reminding President Obama of his promise to end bulk data collection, Franken, a Minnesota Democrat, and Heller, a Nevada Republican, wrote a public letter to the president last week laying out their suggestions. The Senators said the [proposed](https://www.franken.senate.gov/?p=press_release&id=2881" \t "_blank) provisions would:

“Give the American people the information they need to reach an informed opinion about surveillance programs and hold the American government accountable.”

[Introduced](https://beta.congress.gov/bill/113th-congress/house-bill/3361/cosponsors" \t "_blank) by U.S. Rep. James Sensenbrenner, the USA Freedom Act was [originally](http://ivn.us/2013/10/31/usa-freedom-act-introduced-to-limit-nsa-surveillance/?utm_source=ivn&utm_medium=listing_search&utm_campaign=opt-beta-v-1-0" \t "_blank) designed to restore transparency to the process of monitoring suspected American enemies. Many [privacy](http://ivn.us/2014/05/22/privacy-advocates-tech-companies-call-usa-freedom-act-ineffective/?utm_source=ivn&utm_medium=featured&utm_content=title&utm_campaign=opt-beta-v-1-0" \t "_blank) advocates had high hopes for the act.

However, the version that passed the U.S. House was considered watered down to the point that even an original cosponsor, Justin Amash (R-Mich.), [voted against](http://washingtonexaminer.com/justin-amash-votes-against-his-own-bill-the-usa-freedom-act/article/2548767" \t "_blank) it.

The incentive for passing more specific transparency regulations may have become evident in light of recent revelations.

A [report](http://venturebeat.com/2014/06/27/nsa-transparency-report-released/" \t "_blank) from the Office of the Director of National Intelligence revealed the estimated number of people targeted by surveillance agencies. However, the report did not reveal the total number of people who had data collected nor how many of those people were American.

Also, a recently [uncovered](http://apps.washingtonpost.com/g/page/world/fisa-judges-order-authorizing-surveillance-of-foreign-governments-and-organizations/1132/" \t "_blank) 2010 Foreign Intelligence Surveillance Court order [revealed](http://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html" \t "_blank) that a judge gave more extensive power to the NSA than previously thought.

According to the Washington Post, approximately 90 percent of the data collected by the NSA was from people who were not the intended targets. Administration officials have [said](http://www.nytimes.com/2014/07/07/us/officials-defend-nsa-after-new-privacy-details-are-reported.html?_r=0" \t "_blank) that even though the communications of ordinary Internet users are routinely caught in sweeps, those communications get filtered out if they hold no intelligence value.

To explain how these powers can be ambiguous and subject to expansive interpretation, Barton Gellman and Ellen Nakashima [write](http://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html" \t "_blank):

“Language could allow for surveillance of academics, journalists and human rights researchers. A Swiss academic who has information on the German government’s position in the run-up to an international trade negotiation, for instance, could be targeted if the government has determined there is a foreign-intelligence need for that information.”

Debate in the U.S. Senate over the USA Freedom Act is expected to begin sometime this summer. Yet, the most recent revelations about the scope and authority of surveillance may lead to further discussion about its impact on civil liberties within the context of national security.

### Extend privacy rights to EU citizens

Access Now, July 16, 2014, https://www.accessnow.org/blog/2014/07/16/u.s.-may-grant-rights-to-eu-citizens-under-privacy-act

On June 25, U.S. Attorney General Eric Holder announced the Obama administration is seeking to extend to EU citizens several privacy protections in U.S. law, which today are only available to U.S. citizens and permanent residents. If the U.S. Congress follows through and passes legislation to this effect, Europeans will gain access to U.S. courts for certain privacy offences, for the first time.

**First step for EU citizens’ rights**

Holder’s announcement builds on a U.S. Department of Justice [proposal](http://www.justice.gov/opa/pr/2014/June/14-ag-668.html%20) in June to work with Congress to grant EU citizens the same rights to judicial redress as U.S. citizens enjoy under the [Privacy Act of 1974](http://www.law.cornell.edu/uscode/text/5/552a). Currently, if a European user’s information was wrongly disclosed to a U.S. agency, or if a U.S. agency refused to correct errors in a record about them, he or she would have no recourse.

Since 2010, the EU and the U.S. have been negotiating an [Umbrella Agreement](http://europa.eu/rapid/press-release_IP-10-1661_en.htm) on data transfers for criminal law enforcement. The conclusion of this agreement with a mechanism granting judicial redress for EU citizens was [one of the seven objectives](https://www.accessnow.org/blog/2014/02/13/european-parliaments-report-on-nsa-and-gchq-mass-surveillance-activities-pr) laid down in the European Parliament report on the impact of mass surveillance programmes on EU citizens’ fundamental rights. After four years of negotiations, Holder’s announcement might help close this deal, but significant work remains to ensure full protection of the rights of European users.

European authorities [have welcomed](http://europa.eu/rapid/press-release_STATEMENT-14-208_en.htm) Holder’s announcement, seeing it as “an important first step towards rebuilding trust in our transatlantic relations,” and are now waiting for this commitment to be swiftly implemented through legislation.

While Access welcomes the inclusion of a mechanism granting judicial redress for EU citizens in the U.S. in this future agreement, this reform will not end - or even bring transparency to - the wholesale violations of EU citizens’ rights by US surveillance via its top secret intelligence programmes.

… Following this first step to improve the protection of EU citizens’ fundamental right to data protection in the U.S., further reform will be needed in other areas as this new right to judicial redress only applies to information collected for law enforcement purposes.

For instance, this redress would not apply to the Safe Harbour agreement, a data transfer accord between the EU and U.S. meant to facilitate business despite the vast differences in data protection frameworks. By signing up to this agreement, U.S. companies voluntarily adhere to a set of principles in order to demonstrate their compliance with EU data protection standards. This agreement has been the subject of much scrutiny, especially after the NSA disclosures, in particular the [PRISM programme](http://gigaom.com/2014/06/18/facebook-prism-case-heads-to-europes-highest-court/) - an intelligence operation beyond the purview of the Privacy Act.

The EU and the U.S. are currently negotiating a [full review](http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm) of the Safe Harbour, and Access believes this agreement must be significantly strengthened; in its current form, it fails to ensure adequate protection for users’ personal data.

## Specific Plans—Consumer Privacy Protection

### 4 plans

[DM News](mailto:http://www.dmnews.com/amended-privacy-act-could-be-a-boon-to-consumer-trust/article/356833/), June 20

The Direct Marketing Association (DMA) this week issued a statement heralding the news that, by its count, 218 members of the House of Representatives now support efforts to reform the Electronic Communications Privacy Act (ECPA) introduced by Kansas Republican Kevin Yoder. In a floor vote, that number would be enough to pass the amended act in the 435-member House.

Should that occur, the event would cross out No. 4 on DMA's list of five fundamental changes that need to be made in laws regulating free data exchange. Yoder's bill (H.R. 1852) would forbid marketers or other collectors of consumer data to share it with any governmental agency unless backed by a warrant. Government agencies receiving contents of customer communications would be required to notify that customer within three days of receiving the data. Law enforcement agencies would have 10 days. Under the current law, law enforcement can obtain customer data without a warrant 90 days after it is created. Government entities have open access to data after 180 days.

Making it harder for the government to get hold of customer data is an important building block for consumer trust in marketers, says Rachel Nyswander Thomas, executive director of the [Data-Driven Marketing Institute](http://www.dmnews.com/data-driven-marketing-is-a-156-billion-economy/article/316278/) founded last year by DMA. “If we're going to have consumer trust, we need to make sure we are doing due diligence for them,” Thomas says. “There are instances in which DMA feels we should have laws in place to protect consumers, and this is one of them.”

The DMA's other four “Fundamentals for the Future”:

* Pass a national data security and breach notification law
* Pre-empt state laws that endanger the value of data
* Prohibit privacy class action suits and fund FTC enforcement
* Preserve robust self-regulation for the data-driven marketing economy

### Testimony related to protecting consumer financial privacy

[House Financial Services Committee](mailto:http://financialservices.house.gov/calendar/eventsingle.aspx%3FEventID=355849)

**Hearing entitled “Examining Legislative Proposals to Reform the Consumer Financial Protection Bureau”**   
Tuesday, October 29, 2013 3:00 PM in 2128 Rayburn HOB **Financial Institutions and Consumer Credit**

Printed Hearing [113-48](http://financialservices.house.gov/UploadedFiles/113-48.pdf)

Click [here](http://mfile3.akamai.com/65722/wmv/sos1467-1.streamos.download.akamai.com/65726/hearing1029133pm.asx) for the Archived Webcast of this hearing.

Click [here](http://financialservices.house.gov/UploadedFiles/102913_FI_Memo.pdf) for the Committee Memorandum.

**Witness List**

* [Mr. Jess Sharp](http://financialservices.house.gov/UploadedFiles/HHRG-113-BA15-WState-JSharp-20131029.pdf), Executive Director, U.S. Chamber Center for Capital Markets Competitiveness ([TTF](http://financialservices.house.gov/UploadedFiles/HHRG-113-BA15-TTF-JSharp-20131029.pdf))
* [Mr. Robert S. Tissue](http://financialservices.house.gov/UploadedFiles/HHRG-113-BA15-WState-RTissue-20131029.pdf), Senior Vice President and Chief Financial Officer, Summit Financial Group, on behalf of the West Virginia Bankers Association ([TTF](http://financialservices.house.gov/UploadedFiles/HHRG-113-BA15-TTF-RTissue-20131029.pdf))
* [Ms. Lynette Smith](http://financialservices.house.gov/UploadedFiles/HHRG-113-BA15-WState-LSmith-20131029.pdf), President and Chief Executive Officer, Washington Gas Light Federal Credit Union on behalf of the National Association of Federal Credit Unions ([TTF](http://financialservices.house.gov/UploadedFiles/HHRG-113-BA15-TTF-LSmith-20131029.pdf))
* [Mr. Damon A. Silvers](http://financialservices.house.gov/UploadedFiles/HHRG-113-BA15-WState-DSilvers-20131029.pdf), Policy Director and Special Counsel, American Federation of Labor and Congress of Industrial Organizations ([TTF](http://financialservices.house.gov/UploadedFiles/HHRG-113-BA15-TTF-DSilvers-20131029.pdf))

## Specific Plans – 4th Amendment

This area has been debated in both high school and college in the past. Any Supreme Court decisions referenced above (and many more) could be overturned.

## Wording a Resolution

There are a number of things to consider when writing a resolution related to “privacy.”

First, while the area of consumer privacy is interesting, there are not enough arguments (there could be many different plans, but there would be few advantages and disadvantages) to sustain debate on this alone.

The “surveillance” area has similar problems, but not to the same degree. There are more arguments and more interesting arguments related to government surveillance, but there are probably not enough for an independent area.

Second, there are many overlapping argument in the “criminal law” and “surveillance areas,” as many challenge the constitutionality of the many of the surveillance programs on Fourth Amendment grounds.

Third, the “criminal law” area is large enough to independently sustain debate for a year but many of the cases in the area do not capture the core of the recent controversies related to privacy – government mass surveillance and violations of consumer privacy.

Fourth, consideration needs to be given as to whether or not to allow the Affirmative to topically protect/reduce the violations of privacy of individuals, including US citizens, living abroad.

When this 2000 resolution was used, “in the United States” was added after the resolution originally won out of concern that empowering the Affirmative to protect privacy abroad could enable them to do things like make military bases more secure.

*Resolved: That the United States federal government should significantly increase protection of privacy in the United States in one or more of the following areas: employment, medical records, consumer information,* [*search and seizure*](http://en.wikipedia.org/wiki/Search_and_seizure)

As the original advocate for adding “in the United States” to the resolution, I strongly felt that this would create too much Affirmative ground that was not predictable for the Negative. I still largely feel this way, but I think it is important to point out that this time there are reasons to not limit Affirmative plan action to the United States.

(a) US citizens reside both in the US and abroad.  There is a substantial debate in the surveillance literature about protecting the privacy of US citizens abroad and those arguments apply in this context.

(b) The debate about US surveillance of foreigners inside and outside the US is very relevant. There is a considerable amount of evidence that [US spying on countries](http://www.sentinelsource.com/news/national_world/us-in-trouble-for-spying-on-allies/article_47389794-f8a1-525d-9c1c-b61707e2f85a.html) such as [France](http://www.crescent-news.com/ap%20international/2013/10/21/70-3m-records-30-days-nsa-report-draws-paris-ire), [Mexico](http://www.theverge.com/2013/10/20/4858566/nsa-hacked-mexican-presidential-email), Venezuela, Cuba, and Germany have undermined our relations with those countries.   Affirmative teams do not have to defend this practice, however, because it does not part of surveillance of US citizens.

(c) There isn’t a clean separation between foreign and domestic surveillance. For example, how would NSA know who a “foreign” terrorist was communicating with inside the United States unless they could also access domestic meta data?  Exclusively monitoring non-citizen, foreign communications is difficult, and since the goal of many terrorists is to launch attacks inside the United States, and since these attacks likely require communication with (or among) people inside the United States, [monitoring U.S. citizen communications is arguably an inherent part of surveillance designed to prevent a domestic attack](http://prospect.org/article/home-court-advantage).

[*Donald Scarinci*](http://www.scarincihollenbeck.com/attorneys/partners/donald-scarinci/) *is a New Jersey lawyer and managing partner of Scarinci Hollenbeck, LLC a regional law firm with offices in New York, New Jersey and Washington, D.C., April 24, 2014, http://blog.nj.com/njv\_donald\_scarinci/2014/04/is\_the\_nsa\_reading\_your\_emails.html*

**While the NSA’s surveillance efforts are claimed to be targeted at foreigners, a rule change allows NSA analysts to discover and search U.S. citizens’ email, phone calls and databases without a warrant. As long as there is a reasonable belief the communications are foreign and overseas, content and metadata can be collected. The data is being collected under Section 702 of the of the Fisa Amendments Act** (FAA), which gives the NSA authority to target without warrant the communications of foreign targets, who must be non-US citizens and outside the US at the point of collection. However, “**incidental collection” also occurs**. This is the term used to refer to the purely domestic communications that can be inadvertently included in the surveillance sweeps.

Even though the NSA targets foreigners, many Americans are caught up in this surveillance process. [If the US had to stop “non-citizen” surveillance that inherently catches people in this process](http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html), it’s not clear how it could continue to function.

With these considerations in mind, I’ll review a few ways to consider wording the resolution.

*The US federal government should reduce its violations of individual privacy.*

Benefits: Surveillance cases are topical, it’s a way to permit international action without making it too large (it would just reduce direct US surveillance, not protect privacy by enhancing security at foreign military bases)

Problems: Consumer cases are not topical, only a few crime cases are topical because most law enforcement occurs at the state level

*Resolved: That the United States federal government should significantly increase protection of privacy in the United States in one or more of the following areas: surveillance, crime prevention, consumer information.*

Benefits: Includes all core controversies, permits enough crime and consumer information cases (a large majority would be solved by the states counterplan)

Problem: excludes the international debate.

“in the United States” could be excluded from this resolution, but I think that would make the topic too big.

## Benefits to Debating the Topic

It’s very timely.

It’s a good, even debate.

## Concerns with Debating the Topic

Other events (L-D, Public Forum, IPPF) have debated the surveillance portion.

Things change quickly.

## Additional General Background on Privacy

Legally, "privacy" did not come to have meaning in US law until the late 1960s when the Supreme Court said that "right to privacy" covered one's right to marry who one wishes.

Although the Supreme Court used "privacy" to protect this right, the "right to privacy" is not listed anywhere in the Constitution itself.  The Supreme Court actually read privacy into the Constitution (creating a "constitutional right to privacy") by arguing it has a basis in a number of rights, including rights in the First, Third, Fourth, and Ninth amendments.

The First Amendment includes a right to association, which means that people are free to associate with who they want and think what they wish.  The third Amendment says that you do not have to quarter soldiers in your home. The Fourth Amendment says that people are free from unwarranted searches (the court has allowed exceptions) and in the [US v. Katz](http://en.wikipedia.org/wiki/Katz_v._United_States) (1967), the Supreme Court said that freedom is protected when the individual has a legitimate expectation of privacy and when society recognizes that expectation of privacy as legitimate. The Ninth Amendment says that the listing of rights in the Constitution (via Amendment) does not mean that an individual's rights are limited to those specific amendments.

Reading these Amendments together, the Supreme Court said there is a Right to Privacy in the Constitution.  This is a right that they "read into"/"inferred" from the Constitution.

Protections of a "privacy right" can be found more explicitly in some legislation (Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g (2002); Video Privacy Protection Act of 1988, 18 U.S.C. 2701 (2002); Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721-2725 (2002); Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6503 (2002); Privacy Act of 1974, 18 U.S.C. 2510-2522, 2701-2709 (2002); Electronic Communications Privacy Act of 1986, 5 U.S.C. 552a (2002)) and is also protected explicitly in some State Constitutions, such as California's Constitution (In California, the right of privacy is guaranteed by Cal. Const. art. I, § 1, as one of the "inalienable rights" of the people -[California Points & Authorities](https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=18-183+California+Points+%26+Authorities+183.syn&srctype=smi&srcid=2930&key=012657d6c9ba00fe2011181e5dfee6e9))

Although privacy can be defined in many ways, we aren't looking to discuss all possible definitions. Obviously making decisions about one's personal life (using birth control, electing to have an abortion, deciding who to marry) is not at stake here.  Primarily, we are looking at protecting information about oneself and how that information is used.

## Bibliopgrahy – NSA Surveillance (web resources)

**Valuable Papers & Reports**

[The Big Snoop](http://www.brookings.edu/research/essays/2014/big-snoop). A critical read of existing surveillance programs with an easy-to-read history.

[Report to the President — Big Data and Privacy: A Technological Perspective.](http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf)

This report focuses more generally on the question of “big data” and privacy, but it is still useful for some evidence.

[Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies](http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf). This report explores both sides of the privacy/terrorism prevention debate, arguing that current programs should exist but that they should be subject to some basic safeguards and revisions.

[PLCOB Report on the Telephone Records Program](https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf). This report takes a strong stance against the Section 215 metadata collection program, arguing it should be ended.

**Court cases**

[United States v. Jones](http://www.scotusblog.com/case-files/cases/united-states-v-jones/) — This case is more broadly about protecting “metadata” from law enforcement. The decision, briefs, and media analysis are linked here.

[Klayman v. Obama](http://online.wsj.com/public/resources/documents/JudgeLeonNSAopinion12162013.pdf)

**Blogs**

[FISA Reform Lawfare blog](http://www.lawfareblog.com/category/fisa/fisa-reform/)

**Featured SSRN papers**

[The dangers of surveillance](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239412)  
[NSA surveillance since 9/11 and the human right to privacy](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327806)  
[Liberty, Power, and Secret US Surveillance in the US and Europe](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2339338)  
[Surveillance, Human Rights, and international global counterterrorism](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2383976)  
[Human rights treaties and foreign surveillance: privacy in the digital age](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485)  
[Me, my metadata, and the NSA: Privacy and government metada surveillance programs](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2345468)

**Articles**

[Russia’s surveillance state](http://www.worldpolicy.org/journal/fall2013/Russia-surveillance)

**July 23**

[The least known but biggest aspect of NSA surveillance](http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/23/privacy-watchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance/)

[Surveillance reform hinges on changes to Reagan executive order](http://www.theguardian.com/world/2014/jul/23/nsa-surveillance-reform-reagan-order)

[Germany and the NSA are closer than they let on](http://www.dailystar.com.lb/Opinion/Columnist/2014/Jul-24/264888-germany-and-the-nsa-are-far-closer-than-they-let-on.ashx#axzz38LKa697s)

[iPhone back doors can be used for surveillance](http://www.theguardian.com/technology/2014/jul/23/iphone-backdoors-surveillance-forensic-services)

[The German-American break-up](http://www.palmbeachpost.com/news/news/opinion/commentary-the-german-american-breakup/ngkgs/)

[Hard national security choices](http://www.lawfareblog.com/2014/07/todays-headlines-and-commentary-720/)

[Judge rejects call for NSA full disclosure](http://www.courthousenews.com/2014/07/22/69704.htm)

**July 22**

[Like NSA, police spy without warrant](http://www.mintpressnews.com/like-nsa-local-policy-spy-on-americans-without-warrant/194295/)

**July 21**

[New surveillance whistleblower: The NSA violates the Constitution](http://www.theatlantic.com/politics/archive/2014/07/a-new-surveillance-whistleblower-emerges/374722/)

[NSA has access to every iOS device](http://www.dailystar.com.lb/Opinion/Columnist/2014/Jul-24/264888-germany-and-the-nsa-are-far-closer-than-they-let-on.ashx#axzz38LKa697s)

[How spy agencies plan to solve their racism problem](http://www.nationaljournal.com/tech/how-spy-agencies-plan-to-solve-their-racism-problem-20140721)

**July 20**

[Snowden calls on developers to promote privacy](http://vr-zone.com/articles/snowden-calls-developers-promote-privacy/80589.html)

**July 19**

[DropBox is an NSA surveillance target](http://boingboing.net/2014/07/18/snowden-dropbox-is-an-nsa-sur.html)

**July 18**

[‘Be careful,’ working with NSA, US tech security firm warned](http://thehill.com/policy/technology/212526-us-tech-agency-told-to-be-very-careful-with-nsa)

[Meet Executive Order 12333](http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html)

[The NSA’s other privacy loophole](https://www.aclu.org/blog/national-security/nsas-other-privacy-loophole)

**July 17**

[Time running out for NSA surveillance reform](http://www.politico.com/proreport/0714/proreport14664.html)

[Another view: Is NSA keeping too much?](http://www.middletownpress.com/opinion/20140716/another-view-is-nsa-keeping-too-much)

[Snowden claims NSA workers circulate sexually compromising images](http://www.newsweek.com/snowden-claims-nsa-workers-circulate-sexually-compromising-images-targets-259618)

[NSA responds to nude intercept claim](http://www.forbes.com/sites/kashmirhill/2014/07/17/nsa-responds-to-snowden-claim-that-intercepted-nude-pics-routinely-passed-around-by-employees/)

[UN strongly implies NSA surveillance is violating human rights](http://www.vox.com/2014/7/17/5910299/5-ways-obama-may-have-violated-human-rights-according-to-a-un-report)

[A guide to the Edward Snowden anniversary](http://www.diplomaticourier.com/news/topics/security/2306-a-guide-to-the-edward-snowden-anniversary)

[UN: reign in mass surveillance](http://www.eurasiareview.com/18072014-united-nations-rein-mass-surveillance/)

[Hill surveillance reform: time is not on its side](http://www.politico.com/story/2014/07/hill-surveillance-reform-time-109015.html)

**July 16**

[NSA’s online dragnet](http://www.hawaiireporter.com/the-nsas-online-dragnet/123)

[Obama’s failure to reign in the NSA and CIA](http://consortiumnews.com/2014/07/16/obamas-failure-to-rein-in-cia-and-nsa/)

**July 15**

[Germany NSA tools: Typewriters and classical music](http://mashable.com/2014/07/15/germany-typewriters-nsa/)

[Fact checking Pittinger on NSA reform](https://www.aclu.org/blog/national-security/fact-checking-representative-pittenger-nsa-reform)

**July 14**

[Privacy advocates call for FISA court reform](http://time.com/2970766/privacy-freedom-act-reform-secret-nsa-oversight-fisa/)

[UK: Emergency surveillance law a blow to privacy](http://www.trust.org/item/20140715014245-ibzln/)

[NSA: Releasing Snowden emails would violate his privacy](http://www.usnews.com/news/articles/2014/07/14/nsa-releasing-edward-snowden-emails-would-violate-his-privacy)

[Whistleblower: NSA stores 40% of phone calls](http://rt.com/news/172284-nsa-stores-calls-audio/)

[Online polls and other ways British spies seek to control the internet](https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/)

**July 12**

[The government did trash talk our FISA story](https://firstlook.org/theintercept/2014/07/12/yes-government-really-try-undermine-fisa-story-response-washington-post/)

**July 11**

[NSA surveillance compromises internet security](http://www.truth-out.org/news/item/24891-experts-say-nsa-surveillance-compromises-internet-security-heres-how-to-protect-yourself)

**July 10**

[Meet the Muslim leaders the NSA and FBI have been spying on](https://firstlook.org/theintercept/article/2014/07/09/under-surveillance/)

**July 9**

[Racial profiling reported in NSA, FBI surveillance](http://www.usnews.com/news/articles/2014/07/09/racial-profiling-reported-in-nsa-fbi-surveillance)

[FBI’s dirty little secret](http://www.foreignpolicy.com/articles/2014/07/09/the_fbis_dirty_lilttle_secret)

[“Exclusive” on NSA Surveillance reveals nothing new](http://warontherocks.com/2014/07/exclusive-on-nsa-surveillance-reveals-almost-nothing-new/)

[Congress is about to vote on a terrible new cyber security bill](http://www.theverge.com/2014/7/9/5881691/congress-will-vote-on-CISA-controversial-cybersecurity-bill)

**July 6**

[Civil rights organizations demand answers from White House](https://firstlook.org/theintercept/2014/07/09/civil-rights-organizations-demand-answers-white-house-surveillance-muslim-leaders/)

[In NSA intercepted data, those not targeted far outnumber those who are](http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?hpid=z1).

[NSA gathering “startingly intimate’ data on ordinary individuals.](http://rt.com/usa/170708-nsa-target-ordinary-people/)

[NSA intercepts more ordinary user data](http://siouxcityjournal.com/business/columnists/komando/can-the-nsa-spy-on-your-phone-when-it-s/article_b5801b61-8e7c-54a7-8b13-6d4d8be9ffcb.html)

[Can NSA spy on your phone when it is turned off?](http://siouxcityjournal.com/business/columnists/komando/can-the-nsa-spy-on-your-phone-when-it-s/article_b5801b61-8e7c-54a7-8b13-6d4d8be9ffcb.html)

**July 4**

[xKeyscore targeted ordinary users](http://betaboston.com/news/2014/07/03/nsas-xkeyscore-program-targeted-visitors-to-mit-server-tor-project-for-enhanced-scrutiny/)

**July 3**

[Your computer knows and tells all](http://www.cnn.com/2014/07/02/tech/web/digital-evidence/index.html?hpt=hp_c2)

[NSA targets Linux journal](http://www.zdnet.com/nsa-targets-linux-journal-as-extremist-forum-report-7000031241/)

[Edward Snowden and the NSA can’t both be right](http://time.com/2953495/edward-snowden-privacy-nsa/)

**July 2**

[USA privacy panel backs NSA internet tapping](http://www.nytimes.com/2014/07/03/world/privacy-board-backs-nsa-program-that-taps-internet-in-us.html?_r=0)

**June 30**

[NSA monitors entire world](http://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html)

[Court allowed NSA to spy on all but 4 countries](http://techcrunch.com/2014/06/30/court-allowed-nsa-to-spy-on-all-but-4-countries/)

[Legal loopholes could allow wider NSA surveillance](http://www.cbsnews.com/news/legal-loopholes-could-let-nsa-surveillance-circumvent-fourth-amendment-researchers-say/)

[Does cell phone case imperial NSA spying?](http://consortiumnews.com/2014/06/30/does-cell-phone-case-imperil-nsa-spying/)

[FBI, CIA, join NSA in backdoor searches](http://techcrunch.com/2014/06/30/fbi-cia-join-nsa-in-backdoor-searches-on-americans/)

[Senators blast NSA transparency report as lame](http://venturebeat.com/2014/06/30/senators-blast-nsa-transparency-report-as-lame/)

[Transparency report remains controversial](http://voiceofrussia.com/2014_07_01/NSA-new-transparency-teport-nemains-controversial-9976/)

[Tech takes hit from NSA](http://thehill.com/policy/technology/210880-tech-takes-hit-from-nsa)

[NSA spying and the sky not falling](http://www.siliconbeat.com/2014/06/30/quoted-on-nsa-spying-and-the-sky-not-falling/)

[NSA claims to narrow circle of world leaders to surveil](http://voiceofrussia.com/news/2014_07_01/NSA-claims-to-narrow-circle-of-world-leaders-to-surveil-8982/)

[US authorized to spy on BJP](http://www.dnaindia.com/world/report-us-authorised-nsa-to-spy-on-bjp-reveals-edward-snowden-1998854)

**June 28**

[NSA searched more phone numbers last year](http://www.newsmax.com/Newsfront/nsa-phone-search-increase/2014/06/28/id/579808/)

**June 27**

[NSA releases new statistical details on surveillance](http://www.forbes.com/sites/gregorymcneal/2014/06/27/nsa-releases-new-statistical-details-about-surveillance/)

[NSA targeted just 248 Americans](http://rt.com/usa/169016-nsa-targetted-250-americans-2013/)

**June 26**

[Key changes needed to the USA Freedom Act](https://cdt.org/blog/key-changes-needed-to-the-usa-freedom-act-h-r-3361/)

**June 24**

[Greenwald says new NSA leak imminent](http://www.truthrevolt.org/news/glenn-greenwald-new-nsa-leak-snowden-very-imminent)

[House votes to significantly reign in NSA](http://www.infosecurity-magazine.com/view/38984/us-house-votes-to-significantly-rein-in-nsa/)

[International treaties provide loopholes for NSA to spy on Europeans](http://voiceofrussia.com/us/news/2014_06_24/International-treaties-provide-loopholes-for-NSA-to-spy-on-Europeans-0107/)

[House votes to cut funding for NSA surveillance](http://nakedsecurity.sophos.com/2014/06/23/us-house-votes-overwhelmingly-to-cut-funding-of-nsa-surveillance/)

[Government downplaying sensitivity of metadata collection](http://www.mintpressnews.com/government-downplaying-sensitivity-of-metadata-collected-by-nsa/192810/)

[Could big data become big brother?](http://www.govhealthit.com/news/could-big-data-become-big-brother-social-media-LexisNexis#.U6l4go1dVDs)

[Here’s what I tell people who say they don’t care about their privacy — Greenwald](http://www.alternet.org/civil-liberties/glenn-greenwald-heres-what-i-tell-people-who-say-they-dont-care-about-their-privacy)

**June 23**

[NSA granted extension to collect bulk phone data](http://www.pcworld.com/article/2366460/us-nsa-granted-extension-to-collect-bulk-phone-data.html)

**June 21**

[New leak shows Germany’s collusion with NSA](http://www.dw.de/new-leaks-show-germanys-collusion-with-nsa/a-17726141)

[China publishes book on US mass surveillance](http://voiceofrussia.com/news/2014_06_21/China-publishes-146-page-book-on-US-mass-surveillance-3480/)  [Full Text](http://english.peopledaily.com.cn/n/2014/0527/c90883-8732845.html)

**June 16**

[Super secure black phone shipping](http://www.nbcnews.com/tech/mobile/nsa-proof-super-secure-blackphone-shipping-july-n132711)

**June 14**

[Stanford student discredits NSA metadata claims](http://news.stanford.edu/news/2014/june/mayer-engineer-lawyer-061314.html)

[Can NSA spy on your phone when it is turned off?](http://www.komando.com/columns/257659/can-the-nsa-spy-on-your-phone-when-its-turned-off)

**June 13**

[Former NSA director backs bill to reign in agency](http://www.washingtontimes.com/news/2014/jun/12/former-nsa-director-backs-house-bill-rein-agency/)

[Hayden: Ending NSA phone data collection puts US security at risk](http://www.newsmax.com/Newsfront/hayden-nsa-phone-data/2014/06/13/id/576878/)

[New ruling proves NSA can’t legally justify its phone tapping](http://www.wired.com/2014/06/davis-undermines-metadata/)

**June 10**

[NSA: We’re too complex to comply with law](http://boingboing.net/2014/06/10/nsa-were-too-complex-to-com.html)

**June 8**

[A Surveillance State Beyond Imagination Is Being Created in One of the World’s Freest Countries](http://www.alternet.org/civil-liberties/noam-chomsky-surveillance-state-beyond-imagination-being-created-one-freest)

[Capability is tyranny](http://www.forbes.com/sites/davidmarotta/2014/06/08/capability-is-tyranny/)

**June 7**

[Google making it harder for the NSA to get its data](http://time.com/2843295/google-nsa-data/)

[You can fight the NSA](http://journalstar.com/news/opinion/editorial/columnists/column-you-can-fight-the-nsa/article_cfdc884b-5621-5e9a-83d4-9b2cff2805c2.html)

[Empire building, drones, and global surveillance](http://www.delmarvanow.com/story/opinion/columnists/2014/06/07/empire-drones-global/10171419/)

**June 6**

[Governments use secret cables to tap phones](http://www.telegraph.co.uk/technology/internet-security/10880208/Vodafone-governments-use-secret-cables-to-tap-phones.html)

[Senators question need to reign in NSA surveillance](http://www.pcworld.com/article/2360780/senators-question-need-to-rein-in-nsa-surveillance.html)

[Tech company CEOs ask NSA to be reigned in](http://www.bloomberg.com/news/2014-06-05/zuckerberg-nadella-ask-senate-to-restrain-nsa-spying.html)

[How the NSA can turn on your phone remotely](http://money.cnn.com/2014/06/06/technology/security/nsa-turn-on-phone/)

**June 5**

[Reformers frustrated as NSA preserves its powers](http://www.theguardian.com/world/2014/jun/05/edward-snowden-one-year-nsa-surveillance-reform)

[65 things we know about NSA surveillance that we didn’t a year ago](https://www.eff.org/deeplinks/2014/06/65-65-things-we-know-about-nsa-surveillance-we-didnt-know-year-ago)

[Snowden can’t hide the fact that America needs the NSA](http://www.usatoday.com/story/opinion/2014/06/05/nsa-spying-foreign-governments-security-column/9969625/)

[What tech companies still need to do](http://www.slate.com/blogs/future_tense/2014/06/05/snowden_nsa_scandal_anniversary_four_things_tech_companies_still_need_to.html)

**June 4**

[Snowden seeks Brazil asylum](http://www.aljazeera.com/news/americas/2014/06/nsa-whistleblower-snowden-seeks-brazil-asylum-20146451628454409.html)

[NSA Chief: No, we’re not taking pictures of you](http://www.huffingtonpost.com/2014/06/03/nsa-us-photos_n_5439790.html)

[NSA use of facial recognition stays within legal boundary](http://www.bloomberg.com/news/2014-06-03/nsa-use-of-facial-recognition-stays-within-legal-boundary.html)

[The real cost of NSA surveillance](http://www.cnn.com/2014/06/04/opinion/kehl-bankston-nsa-surveillance/)

**June 3**

[Another judge upholds NSA call tracking](http://www.politico.com/blogs/under-the-radar/2014/06/another-judge-upholds-nsa-call-tracking-189671.html?hp=r2)

[NSA reforms go a bit too far](http://thehill.com/policy/technology/208086-chambliss-house-nsa-reforms-go-a-little-bit-too-far)

[Five dumbest ways people defend NSA spying](http://gizmodo.com/the-five-dumbest-ways-that-people-defend-nsa-spying-1585242095)

[Federal government destroyed evidence of  electronic spying](http://www.mintpressnews.com/federal-government-knowingly-destroyed-evidence-of-electronic-spying/191820/)

**June 2**

[Reddit, Boing Boing launch anti-NSA campaign](http://www.theguardian.com/technology/2014/jun/02/reddit-imgur-boing-boing-reset-the-net-campaign-nsa-surveillance-privacy)

[NSA steps up digital image harvesting](http://www.foxnews.com/politics/2014/06/01/nsa-steps-up-digital-image-harvesting-to-feed-its-advancing-facial-recognition/)

[House Intel Committee ignores report calling NSA surveillance illegal](http://www.openmarket.org/2014/06/02/house-intel-committee-chair-ignores-report-calling-nsa-surveillance-illegal/)

**May 31**

[NSA collecting millions of Faces from web pages](http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?smid=fb-share&_r=0)

[Millions of images per day collected from intercepted communications](http://www.theblaze.com/stories/2014/05/31/nsa-gathering-millions-of-images-per-day-from-intercepted-communications-ny-times-reports/)

**May 30**

[NSA releases Snowden email exchange](http://www.cnn.com/2014/05/29/politics/snowden-nsa-email/)

[It may be the time to get off the cloud](http://www.dnaindia.com/lifestyle/report-it-may-be-the-time-to-get-off-that-cloud-1992678)

**May 29**

[Privacy under attack: NSA files reveal new threats to democracy](http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy)

**May 27**

[NSA aims for absolute surveillance](http://www.itweb.co.za/index.php?option=com_content&view=article&id=134825)

[Greenwald to release list of Americans under NSA surveillance](http://boingboing.net/2014/05/27/greenwald-to-release-list-of-a.html)

[Google’s Brin says NSA snooping was a huge dissapointment](http://www.cnbc.com/id/101708672)

**May 25**

[Snowden considers return to US](http://rt.com/news/161396-snowden-conditions-return-usa/)

[Surveillance issues abound on Facebook’s microphone data collection scheme](http://www.investing.com/news/stock-market-news/surveillance-issues-abound-on-facebook%27s-microphone-data-collection-scheme-286143)

**May 24**

[USA surveillance recording almost every phone call in Afghanistan](http://www.business-standard.com/article/news-ani/us-surveillance-program-recording-almost-every-phone-call-in-afghanistan-wikileaks-114052400430_1.html)

[China v. America’s cyber hegemony](http://www.panorama.am/en/politics/2014/05/24/eric-draitser/)

**May 23**

[Police state America mostly spies on its own](http://mwcnews.net/focus/politics/41017-america-spies.html)

[It’s time for America to scale back its surveillance](http://www.concordmonitor.com/home/12076097-95/my-turn-its-time-for-america-to-scale-back-surveillance)

**May 22**

[NSA surveilling Philippines with MYSTIC program](http://www.rappler.com/technology/news/58668-nsa-mystic-spying-bahamas-philippines)

[Surveillance state: the NSA doesn’t stand alone](http://boingboing.net/2014/05/21/surveillance-state-the-nsa-do.html)

[White House authorized spying on OSCE](http://en.ria.ru/world/20140522/190036586/White-House-Authorized-NSA-Spying-on-OSCE--Report.html)

[Facebook, Google says bill falls short](http://www.livemint.com/Industry/dlejGEprg1OgUwjfn1ilDI/Facebook-Google-say-Bill-to-curb-NSA-spying-falls-short.html)

**May 21**

[Are cloud providers facing a backlash?](http://cloudtweaks.com/2014/05/cloud-providers-facing-backlash-continued-nsa-revelations/)

[Greenwald: Washington Post “suppressed” foreign countries operating under NSA surveillance](http://www.washingtonpost.com/blogs/erik-wemple/wp/2014/05/20/greenwald-washington-post-suppressed-foreign-countries-under-nsa-eavesdropping-program/?wpisrc=nl_opinions)

[Restrictions placed on NSA’s data store.](http://www.theguardian.com/world/2014/may/20/nsa-reform-restrictions-data-surveillance-talks)

[NSA snooping isn’t just a privacy problem](http://www.thefiscaltimes.com/Articles/2014/05/21/NSA-Snooping-Isn-t-Just-Privacy-Problem)

[How the NSA is targeting law enforcement](http://gizmodo.com/how-the-nsa-is-transforming-law-enforcement-1579438984)

[Wikileaks threatens to name NSA target countries](http://macedoniaonline.eu/content/view/25336/56/)

[Australia secretly spies on the Phillipines](http://au.ibtimes.com/articles/553162/20140521/edward-snowden-nsa-spying-australia-philippines.htm)

[Amash takes on the NSA](http://personalliberty.com/amash-takes-nsa/)

[House Committee guts key provisions in NSA reform bill](http://www.huffingtonpost.com/2014/05/20/house-rules-nsa_n_5360978.html)

**May 20**

[NSA is recording *every call* in the Bahamas](http://www.gizmodo.in/science/Report-NSA-Is-Recording-Every-Call-in-the-Bahamas-Including-Oprahs/articleshow/35352290.cms)  — [Original report](https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/)

[‘New evidence’ emerges about NSA surveillance plans](http://www.techradar.com/news/internet/web/new-evidence-emerges-about-nsa-extensive-surveillance-plans-1249641)

[Only email system NSA can’t access](http://english.farsnews.com/newstext.aspx?nn=13930230001209)

[NSA data mining may run into a California road block](http://www.reuters.com/article/2014/05/20/us-usa-california-spying-idUSBREA4J02I20140520)

[Progressives are missing on the surveillance state](http://www.washingtonpost.com/opinions/katrina-vanden-heuvel-progressives-are-missing-on-the-surveillance-state/2014/05/19/6e71f65c-ded6-11e3-8dcc-d6b7fede081a_story.html)

**May 19**

[Cisco chief urges Obama to limit surveillance activity](http://www.reuters.com/article/2014/05/18/us-cisco-systems-nsa-idUSBREA4H0C720140518)

[No Place to Hide review](http://www.theguardian.com/books/2014/may/19/no-place-to-hide-review-glenn-greenwald-nsa-gchq-surveillance-edward-snowden-spying)

[NSA’s future rests on Admiral Roger’s shoulders](http://www.globalpost.com/dispatch/news/thomson-reuters/140519/post-snowden-the-nsas-future-rests-admiral-rogers-shoulders)

[Advocates Warn NSA Reform Gutted](http://news.antiwar.com/2014/05/18/advocates-warn-nsa-reform-gutted/)

**May 18**

[Feinstein blasts critics of NSA program](http://thehill.com/policy/technology/206434-a-surveillance-program-or-not)

[Can the surveillance state be stopped?](http://consortiumnews.com/2014/05/18/can-the-surveillance-state-be-stopped/)

[There is no privacy — get over it](http://www.news-gazette.com/opinion/guest-commentary/2014-05-18/voices-there-no-privacy-get-over-it.html)

**May 17**

[NSA allegedly planted “beacons” into servers](http://austriantribune.com/informationen/143636-nsa-allegedly-planted-beacons-servers-routers-and-other-network-gear-prior)

[Spring was the only telco to stand up to the US](http://venturebeat.com/2014/05/16/sprint-was-the-only-telco-to-stand-up-to-the-nsa/)

**May 16**

[Microsoft openly offered cloud data to the NSA](http://betanews.com/2014/05/16/microsoft-openly-offered-cloud-data-to-the-nsa/)

Microsoft cooperates/cooperated with the NSA to enable the NSA to access its cloud data storage systems

Betanews, May 16, 2014, http://betanews.com/2014/05/16/microsoft-openly-offered-cloud-data-to-the-nsa/

Microsoft’s cooperation with the NSA and FBI on the controversial Prism program has been laid bare in a new book written by an American journalist who brought it to public attention in the first place. Glenn Greenwald, the American journalist who worked extensively with Edward Snowden, wrote in a new book that Microsoft’s cloud services allowed the National Security Agency [NSA] to collect data from a range of its different cloud options. “Beginning on 7 March 2013, Prism now collects Microsoft SkyDrive data as part of Prism’s standard Store Communications collection package for a tasked FISA Amendments Act Section 702 [FAA702] selector,” stated a slide released by Greenwald, according to [Cloud Pro](http://www.cloudpro.co.uk/cloud-essentials/cloud-security/4123/nsa-documents-show-microsofts-prism-cooperation). It is detailed in Greenwald’s new book, No Place to Hide: Edward Snowden, the NSA and the Surveillance State, and goes on to hint that Microsoft was implicit in the NSA data collecting process. “This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established,” the document stated. Part of the reason that it was able to do this was down to the FISA Amendment Act of 2008 that legalized NSA Internet surveillance and allowed warrantless wiretapping by the NSA and related agencies. “This means that analysts will no longer have to make a special request to SSO for this. This new capability will result in a much more complete and timely collection response from SSO for our enterprise customers,” the documents added.

NSA engages in electronic supply-chain interdiction

Betanews, May 16, 2014, http://betanews.com/2014/05/16/microsoft-openly-offered-cloud-data-to-the-nsa/

Other sabotage methods employed by the NSA and outlined in Greenwald’s book include the supply-chain interdiction, which meant intercepting various communications products in order to carry out covert surveillance. This included routers and servers made by Cisco and involved implanting beacons before the products were repackaged and shipped out to customers across the world. “While American companies were being warned away from supposedly untrustworthy Chinese routers, foreign organizations would have been well advised to beware of American-made ones,” Greenwald said.

[Amazon and Snapchat rank low for protecting user data from the government](http://www.theguardian.com/world/2014/may/16/amazon-snapchat-data-eff-privacy-nsa-government-snowden)

Amazon and Snapchat will turn over data without a warrant

Samuel Gibbs, May 16, 2014, http://www.theguardian.com/world/2014/may/16/amazon-snapchat-data-eff-privacy-nsa-government-snowden

Amazon and Snapchat rank among the worst at protecting your data from government requests, according to a US privacy pressure group. The Electronic Frontier Foundation (EFF) publishes [Who Has Your Back?](https://www.eff.org/who-has-your-back-government-data-requests-2014) report annually, analysing the activity of companies ordered to hand over sensitive user data in response to US government requests. The report finds huge variation in the lengths technology companies will go to to protect their users. Nate Cardozo, a lawyer for EFF, said in a statement: “Snapchat joins AT&T and Comcast in failing to require a warrant for government access to the content of communications. That means the government can obtain extraordinarily sensitive information about your activities and communications without convincing a judge that there is probable cause to collect it.” Snapchat was awarded one star out of six in the EFF’s report, solely for publishing guidelines for law enforcement requests. The ephemeral messaging service was [recently reprimanded by the US Federal Trade Commission](http://www.theguardian.com/technology/2014/may/08/snapchat-ftc-false-claims-messaging-service) for the collection of personal data and false claims that messages “disappear forever”. A Snapchat spokeswoman said the company required search warrants, but that the ephemerality of the service meant that there was often no data to release. Amazon was awarded two stars. It does, however, require a warrant to hand over user data, and was praised for repeatedly fighting in court to protect the privacy of its users’ book purchases. Amazon did not respond to a request for comment.

[Who owns your personal data?](http://www.newsobserver.com/2014/05/16/3867496/drescher-who-owns-your-personal.html)

[Can we stop the American surveillance state?](http://www.huffingtonpost.com/danny-schechter/can-we-stop-americas-surv_b_5334572.html?utm_hp_ref=politics&ir=Politics)

[NSA data collection unconstitutional](http://www.seacoastonline.com/apps/pbcs.dll/article?AID=/20140516/OPINION/405160373/-1/NEWSMAP)

[NSA spying reforms fail to satisfy experts](http://www.reuters.com/article/2014/05/16/us-cyber-summit-reforms-idUSBREA4F0MX20140516)

NSA continues to exploit software vulnerabilities for spying purposes

Joseph Menn, Reuters, May 16, 2014, “Obama’s spying reforms fail to satisfy experts,” http://www.reuters.com/article/2014/05/16/us-cyber-summit-reforms-idUSBREA4F0MX20140516

Obama administration actions to change some of the National Security Agency’s surveillance `practices after the leaks of classified documents by contractor Edward Snowden are falling short of what many private cyber experts want. Top government experts told the Reuters Cybersecurity Summit this week they would be more transparent about spying activity. Non-government guests, however, said the administration was not doing enough to advance Internet security. For instance, last December a White House review commission called for a drastic reduction in the NSA’s practice of keeping secret the [software](http://www.reuters.com/sectors/industries/overview?industryCode=174&lc=int_mb_1001) vulnerabilities it learns about and then exploiting them for spying purposes. White House cybersecurity advisor Michael Daniel said at the conference that he would chair the interagency group charged with weighing each newly discovered [software](http://www.reuters.com/sectors/industries/overview?industryCode=174&lc=int_mb_1001) flaw and deciding whether to keep it secret or warn the software maker about it. “The policy has been in place for a number of years, but it was not as active as we decided that it should be,” Daniel said. Now, he said, “there is a process, there is rigor in that process, and the bias is very heavily tilted toward disclosure.” Commission member Peter Swire told the summit he was pleased by the formal process for debating vulnerability use, but others said there were too many loopholes. In an April 28 White House blog post, Daniel wrote that the factors the interagency group would consider included the likelihood that the vulnerability would be discovered by others and how pressing was the need for intelligence. “That is the loophole that swallows the entire policy, because there’s always going to be an important national security or law enforcement purpose,” Chris Soghoian, a technology policy analyst with the American Civil Liberties Union said at the summit. Some security experts active in the market for trading software flaws said they had seen no sign that U.S. purchases were declining. “There’s been no change in the market at all as far as we can see,” said Adriel Desautels, chief executive of Netragard Inc, which buys and sells programs taking advantage of undisclosed flaws.

[The right to be forgotten](http://www.scmagazineuk.com/icymi-the-right-to-be-forgotten-nsa-transparency-and-security-nativity/article/347279/)

[Collect it all, then what?](http://www.thedailybeast.com/articles/2014/05/16/the-nsa-can-collect-it-all-but-what-will-it-do-with-our-data-next.html)

**May 15**

[General Keith Alexander interview](http://www.newyorker.com/online/blogs/newsdesk/2014/05/were-at-greater-risk-q-a-with-general-keith-alexander.html)

[Papers: Telecom questioned NSA surveillance](http://www.click2houston.com/news/Papers-Telecom-questioned-NSA-surveillance/25987610)

[How FBI & NSA made Facebook the perfect surveillance tool](http://venturebeat.com/2014/05/15/how-the-nsa-fbi-made-facebook-the-perfect-mass-surveillance-tool/)

FBI & NSA develop individual profiles through Facebook exploitation

Harrison Weber, May 15, 2014, “How the NSA & FBI Made Facebook the Perfect Surveillance Tool,” Venture Beat, http://venturebeat.com/2014/05/15/how-the-nsa-fbi-made-facebook-the-perfect-mass-surveillance-tool/  
The National Security Agency and the FBI teamed up in October 2010 to develop techniques for turning Facebook into a surveillance tool. Documents [released alongside](http://glenngreenwald.net/#BookDocuments) security journalist Glenn Greenwald’s new book, “No Place To Hide,” reveal the NSA and FBI partnership, in which the two agencies developed techniques for exploiting Facebook chats, capturing private photos, collecting IP addresses, and gathering private profile data. According to the slides below, the agencies’ goal for such collection was to capture “a very rich source of information on targets,” including “personal details, ‘pattern of life,’ connections to associates, [and] media.” NSA documents make painfully clear how the agencies collected information “by exploiting inherent weaknesses in Facebook’s security model” through its use of the popular [Akamai](http://www.akamai.com/) content delivery network. The NSA describes its methods as “assumed authentication,” and “security through obscurity.” The slide below shows how the NSA and U.K. spy agency GCHQ also worked together to “obtain profile and album images.” Two months ago, following a series of Facebook-related NSA spying leaks, Facebook chief Mark Zuckerberg stated in a [blog post](https://www.facebook.com/zuck/posts/10101301165605491) that he’s “confused and frustrated by the repeated reports of the behavior of the U.S. government.” According to [a report by](https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/)The Intercept, the above slides do not reveal the NSA’s Facebook surveillance program in full. The report states that the NSA also “disguises itself as a fake Facebook server” to perform “[man-in-the-middle](https://en.wikipedia.org/wiki/Man-in-the-middle)” and “man-on-the-side” attacks and spread malware.

**May 14**

[The official US position is still unlimited eavesdropping](http://www.theguardian.com/commentisfree/2014/may/14/nsa-eavesdropping-program-constitutional)

[Many more NSA revelations to come](http://www.thedrum.com/news/2014/05/15/many-more-nsa-revelations-come-glenn-greenwald-tells-al-jazeera-snowden-very-happy-0)

[A conservative critique of the radical NSA](http://www.theatlantic.com/politics/archive/2014/05/on-nsa-surveillance-glenn-greenwald-is-not-the-radical/370830/)

[NSA metadata, abuse Americans rights](http://www.presstv.ir/detail/2014/05/14/362621/nsa-metadata-abuse-of-us-public-rights/)

**May 13**

[NSA gave Canada money for surveillance program](http://www.huffingtonpost.ca/2014/05/13/nsa-canada-money-glenn-greenwald-book_n_5317673.html)

Michael Bolen, Huffington Post, May 13, 2014, “NSA Gave Canada Money for Surveillance Program,” http://www.huffingtonpost.ca/2014/05/13/nsa-canada-money-glenn-greenwald-book\_n\_5317673.html

The National Security Agency paid Canada to help develop its surveillance capabilities, according to [documents](http://glenngreenwald.net/pdf/NoPlaceToHide-Documents-Compressed.pdf) published by Glenn Greenwald in a new book. In [“No Place To Hide”](http://www.amazon.ca/No-Place-Hide-Snowden-Surveillance/dp/0771036787), Greenwald, the journalist who has been the conduit for the Edward Snowden leaks, reveals that Canada was the fourth largest recipient of money in 2012 from an NSA program aimed at helping partner nations cover “R&D and technology costs.” Only Pakistan, Jordan and Ethiopia received more funding. The document does not provide an exact sum but suggests Canada received somewhere between $300,000 and $400,000 in 2012. The book also provides insight into how the NSA views its relationship with Canada’s electronic surveillance agency CSEC. In a redacted document, the NSA details how it co-operates with CSEC in “targeting approximately 20 high-priority countries.” The specific nations are not included and the section following the statement is blacked out. The document also notes what CSEC gives the NSA, including opening “covert sites at the request” of the U.S. agency and sharing its “unique geographic access to areas unavailable to the U.S.” CSEC is not supposed to spy on Canadians but has [admitted that it sometimes “incidentally” monitors citizens](http://www.huffingtonpost.ca/2014/01/07/csec-spying-canada_n_4555873.html). The new documents raise questions about how much data intercepted in Canada is being shared with the NSA. Canada is a member of the surveillance alliance known as the Five Eyes, which includes the U.S., U.K., Australia and New Zealand. In an NSA document from “No Place To Hide” the group is characterized as taking part in “comprehensive cooperation.”

[NSA installing spyware on US-made hardware](http://washington.cbslocal.com/2014/05/13/report-nsa-installing-spyware-on-us-made-hardware/)

Government installing spyware on hardware

CBS Local, May 13, 2014, http://washington.cbslocal.com/2014/05/13/report-nsa-installing-spyware-on-us-made-hardware/

The National Security Agency has been accessing routers, servers and other computer network devices to plant backdoors and other spyware before the hardware is shipped overseas, reports [CNET](http://www.cnet.com/news/nsa-reportedly-installing-spyware-on-us-made-hardware/). The accusation is at the heart of a new book from journalist Glenn Greenwald. In “No Place to Hide,” Greenwald details documents obtained from NSA leaker Edward Snowden that show how the NSA is intercepting devices in the U.S. before they are exported. According to [The Guardian](http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden), the report details how the NSA allegedly intercepted American-made [hardware](http://washington.cbslocal.com/2014/05/13/report-nsa-installing-spyware-on-us-made-hardware/), embedded backdoor surveillance tools, then repackaged the equipment and sentg it onto international customers. With such backdoor surveillance systems in place, the NSA could conceivably gain access to almost any global computer network. “In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert [infrastructure](http://washington.cbslocal.com/2014/05/13/report-nsa-installing-spyware-on-us-made-hardware/),” the NSA report says, according to the Guardian. “This call back provided us access to further exploit the device and survey the network”

[NSA accused of installing backdoors in US tech exports](http://www.infosecurity-magazine.com/view/38391/nsa-accused-of-installing-backdoors-on-us-tech-exports/)

Info Security Magazine, May 14, 2014, “NSA accused of installing back-doors on US tech exports” <http://www.infosecurity-magazine.com/view/38391/nsa-accused-of-installing-backdoors-on-us-tech-exports/>

The new head of the US National Security Agency vowed on Monday to bring greater transparency to the under-fire spy agency, but his words were undermined by newly released allegations claiming the NSA routinely intercepted US-made routers bound for export and planted backdoors on them. The allegations appear to be based on yet more information gleaned from the treasure trove of secret documents lifted by [Edward Snowden](http://www.infosecurity-magazine.com/view/37130/snowden-to-testify-before-european-parliaments-libe-committee) and soon to be published in a book by journalist Glenn Greenwald. They include a June 2010 report from the head of the NSA’s Access and Target Development department which claims the agency either receives or intercepts servers, routers and other tech kit bound for international customers, according to an excerpt in [*The Guardian*](http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden). The NSA then fits the kit with some kind of backdoor surveillance tool before repackaging the gear and replacing the factory seal, Greenwald alleges.

[NSA spying on foreign embassies](http://www.tasnimnews.com/English/Home/Single/369037)

Tasmin News, May 13, 2014, “NSA Spying on Foreign Embassies Helped US “Develop” Strategy, http://www.tasnimnews.com/English/Home/Single/369037

In May 2010, as the UN Security Council was attempting to win support for sanctions against Iran over its nuclear-energy program, several members were undecided as to how they would vote. At this point, the US ambassador to the world body, Susan Rice, asked the NSA for assistance in her efforts to “develop a strategy,” leaked NSA documents reveal. The NSA swung into action, aiming their powerful surveillance apparatus at the personal communications of diplomats from four non-permanent Security Council members — Bosnia, Gabon, Nigeria and Uganda. This gave Rice an apparent upper-hand in the course of the negotiations, RT reported.

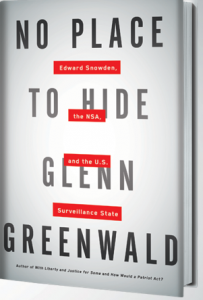
In June, 12 of the 15-member Security Council voted in favor of new sanctions.

Later, Rice extended her gratitude to the US spy agency, saying its surveillance had helped her to know when diplomats from the other permanent representatives — China, England, France and Russia — “were telling the truth … revealed their real position on sanctions … gave us an upper hand in negotiations … and provided information on various countries’ ‘red lines’.” The information comes from a new book by journalist Glenn Greenwald, ‘No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State’, the New York Times reported. Rice’s request for assistance was discovered in an internal report by the security agency’s Special Source Operations division, which cooperates with US telecommunications companies in the event a request for information is deemed necessary.

[Greenwald releases more NSA documents](http://www.theverge.com/2014/5/13/5713092/glenn-greenwald-releases-more-nsa-documents-along-with-new-book)

Today, Glen Greenwald’s new book, “[No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State](http://www.amazon.com/gp/product/B00E0CZX0G/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&camp=1789&creative=9325&creativeASIN=B00E0CZX0G&linkCode=as2&tag=npth-20&linkId=MB6MZYHWN2BOLYH7),” was released. The book contains an account of his meetings with Snowden and some new revelations (see the information above in this post) about NSA spying.

All of the documents in the book, the book notes, and some other information are available [here.](http://glenngreenwald.net/#BookDocuments)

[](http://bauscharddebate.com/wp-content/uploads/2014/04/Screen-Shot-2014-05-18-at-5.56.39-AM.png)

**May 12**

[New NSA chief vows more transparency](http://in.reuters.com/article/2014/05/12/uk-cyber-summit-nsa-rogers-idINKBN0DS1MF20140512)

New NSA head supports current programs, just says they need to be better explained

Reuters, May 12, 2014, http://in.reuters.com/article/2014/05/12/uk-cyber-summit-nsa-rogers-idINKBN0DS1MF20140512

The new head of the National Security Agency vowed on Monday to lead the embattled spy agency with greater transparency as it balances individual rights against the rising risk of a destructive cyber attack against the United States. In his first interview since taking the helm of both the NSA and U.S. Cyber Command in April, Admiral Mike Rogers said he would be more candid with the public about much of the NSA’s work after nearly a year of damaging revelations by former NSA contractor Edward Snowden. But he also staunchly defended the NSA’s controversial electronic surveillance programs, emphasizing that they were legal and needed better explanation rather than an overhaul. “It is by design that I have tried to start a series of engagements with a broader and perhaps more different groups than we have traditionally done,” Rogers told the Reuters Cybersecurity Summit in Washington.

[NSA believes it should be able to monitor all communication](http://www.ktoo.org/2014/05/12/glenn-greenwald-nsa-believes-able-monitor-communication/)

**May 11**

[Here’s how you can resist the NSA](http://www.thedailybeast.com/articles/2014/05/12/crypto-for-the-masses-here-s-how-you-can-resist-the-nsa.html)

**May 10**

[The battle to retake our privacy can be won](http://www.theguardian.com/commentisfree/2014/may/10/the-battle-to-retake-our-privacy-can-be-won-in-the-halls-of-congress-really)

**May 9**

[House compromises on NSA reform](http://www.csmonitor.com/USA/DC-Decoder/2014/0509/House-compromise-on-NSA-reform-how-it-balances-freedom-and-security-video)

**May 8**

[NSA spy program one stop closer to extinction](http://www.newsmax.com/Newsfront/NSA-surveillance-House-Senate/2014/05/08/id/570169/)

[The way the NSA uses Section 702 is deeply troubling](http://www.rightsidenews.com/2014050834239/us/homeland-security/the-way-the-nsa-uses-section-702-is-deeply-troubling-here-s-why.html)

Right Side News, May 8, 2014, “The Way the NSA Uses Section 702 is Deeply Troubling,” http://www.rightsidenews.com/2014050834239/us/homeland-security/the-way-the-nsa-uses-section-702-is-deeply-troubling-here-s-why.html

Section 702 has been used by the NSA to justify mass collection of phone calls and emails by collecting huge quantities of data directly from the physical infrastructure of communications providers. Here’s what you should know about the provision and why it needs to be addressed by Congress and the President:

* Most of the discussion around the NSA has focused on the phone records surveillance program. Unlike that program, collection done under Section 702 [captures](https://www.eff.org/deeplinks/2013/07/what-it-means-be-target-or-why-we-once-again-stopped-believing-government-and-once) **content of communications**. This could include content in emails, instant messages, Facebook messages, web browsing history, and more.
* Even though it’s ostensibly used for foreign targets, Section 702 surveillance indiscriminately **sweeps up everyone’s communication, including the** [**communications of Americans**](https://www.eff.org/deeplinks/2013/07/what-it-means-be-target-or-why-we-once-again-stopped-believing-government-and-once)**.** The NSA has a twisted, and incredibly permissive, interpretation of targeting. As John Oliver put it in his [interview](https://www.youtube.com/watch?v=k8lJ85pfb_E) with former NSA General Keith Alexander: “No, the target is not the American people, but it seems that too often you miss the target and hit the person next to them going, ‘Whoa, him!’”
* The NSA has confirmed that it is searching Section 702 data to **access American’s communications without a warrant**, in what is being called the “back door search loophole.”  In response to questions from Senator Ron Wyden, former NSA director [General Keith Alexander admitted](http://www.wyden.senate.gov/news/press-releases/wyden-udall-on-revelations-that-intelligence-agencies-have-exploited-foreign-intelligence-surveillance-act-loophole) that the NSA specifically searches Section 702 data using “U.S. person identifiers,” for example email addresses associated with someone in the U.S.
* The NSA has used Section 702 to justify **programs like PRISM,** allowing the NSA to “[siphon off](https://www.eff.org/deeplinks/2013/08/illustration-how-nsa-misleads-public-without-actually-lying) large portions of Internet traffic directly from the Internet backbone.” PRISM exploits the structure of the Internet, in which a significant amount of traffic from around the world flows through servers in the United States. According to the Washington Post, it gives the NSA [direct access to servers](http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/) of major American companies like Facebook and Google.
* Section 702 is likely used for [computer warfare](http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html), including activities targeting computers in the United States. We know that the **NSA’s hacking outfit**, the [Tailored Access Operations Unit](https://www.eff.org/deeplinks/2014/03/new-nsa-slides-reveal-tailored-access-run-amok), needs information like that collected by PRISM to function, and Richard Ledgett, Deputy Director of NSA, [noted](https://web.archive.org/web/20140323232303/http:/http:/www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk) the use of intelligence authorities to mitigate cyber attacks.
* The FISA Court has [little opportunity to review](https://www.eff.org/deeplinks/2014/04/eff-privacy-and-civil-liberties-oversight-board-stop-mass-collection-innocent) Section 702 collection. The court approves procedures for 702 collection for up to a year. This is not approval of specific targets, however; “court review [is] limited to ‘procedures’ for targeting and minimization rather than the actual seizure and searches.” This **lack of judicial oversight** is far beyond the parameters of criminal justice.
* Not only does the FISA Court provide little oversight, **Congress is largely in the dark about Section 702** collection as well. [NSA spying defenders](http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/) say that Congress has been briefed on these programs. But other members of Congress have repeatedly noted that it is incredibly [difficult to get answers](https://firstlook.org/theintercept/2014/03/05/congress-intelligence-community-whos-overseeing/) from the intelligence community, and that attending classified hearings means being unable to share any information obtained at such hearings. What’s more, as Senator Barbara Mikulski stated: “‘Fully briefed’ doesn’t mean that we know what’s going on.”  Without a full picture of Section 702 surveillance, Congress simply [cannot provide oversight](http://www.politico.com/story/2014/03/hill-draws-criticism-over-nsa-oversight-104151.html).
* Section 702 is **not just about keeping us safe from terrorism**. It’s a distressingly powerful surveillance tool. While the justification we’ve heard repeatedly is that NSA surveillance is keeping us safer, data collected under Section 702 [can be shared](https://www.eff.org/deeplinks/2013/11/nsas-surveillance-powers-extend-far-beyond-terrorism-despite-governments) in a variety of circumstances, such as ordinary criminal investigations. For example, the NSA has [shared intelligence](https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering) with the Drug Enforcement Agency that has led to prosecutions for drug crimes, all while concealing the source of the data.
* Much like most of the [legislation](https://www.eff.org/deeplinks/2014/04/making-sure-nsa-reform-isnt-caught-gears-dc-machine) that Congress has proposed to fix NSA spying, the **President has largely ignored Section 702.** While Section 215 of FISA has received significant attention from President Obama, in his [speeches](https://www.eff.org/deeplinks/2014/01/rating-obamas-nsa-reform-plan-eff-scorecard-explained) and his most [recent proposal](https://www.eff.org/deeplinks/2014/03/eff-statement-proposals-overhaul-nsa-spying), Section 702 remains nearly [untouched](https://www.eff.org/deeplinks/2014/01/presidents-review-group-puzzler-why-mass-surveillance-wrong-under-215-ok-under).
* The way the NSA uses Section 702 is **illegal and unconstitutional**—and it violates [international human rights law](https://en.necessaryandproportionate.org/about). Unlike searches done under a search warrant authorized by a judge, Section 702 has been used by the NSA to get broad FISA court authorization for [general search and seizure](https://www.eff.org/document/eff-pclob-section-702-comments) of huge swathes of communications. The NSA says this is OK because Section 702 targets foreign citizens. The problem is, once constitutionally protected communications of Americans are swept up, the NSA says these communications are “fair game” for its use.
* Innocent **non-Americans don’t even get the limited and much abused protections the NSA promises for Americans**. Under international human rights law to which the United States is a signatory, the United States must respect the rights of all persons. With so many people outside the United States keeping their data with American companies, and so much information being swept up through mass surveillance, that makes Section 702 the loophole for the NSA to violate the privacy rights of billions of Internet users worldwide.

The omission of Section 702 reform from the discourse around NSA surveillance is incredibly concerning, because this provision has been used to justify some of the most invasive NSA surveillance. That’s why EFF continues to push for real reform of NSA surveillance that includes an end to Section 702 collection. You can help by educating yourself and engaging your elected representatives. Print out our handy [one-page explanation](https://www.eff.org/document/702-one-pager-adv) of Section 702. [Contact](https://action.eff.org/o/9042/p/dia/action/public/?action_KEY=9601) your members of Congress today and tell them you want to see an end to all dragnet surveillance, not just bulk collection of phone records.

[Putin to Russian bloggers: You now operate at my discretion](http://venturebeat.com/2014/05/07/putin-to-russian-bloggers-you-now-operate-at-my-discretion/)

[Google and the NSA are pretty cozy](http://www.bustle.com/articles/23633-google-the-nsa-are-pretty-cozy-as-it-turns-out)

NSA and big tech company CEOs were cooperating

Caitlin Mahon, May 12, 2014, “Google and the NSA are pretty cozy, as is turns out” Bustle, http://www.bustle.com/articles/23633-google-the-nsa-are-pretty-cozy-as-it-turns-out

Even big technology companies grilled President Barack Obama in late 2013 about the NSA surveillance programs, leading many to believe they knew nothing about it or only acted when they absolutely had to by law. Except, [this isn’t exactly true.](http://america.aljazeera.com/articles/2014/5/6/nsa-chief-google.html)

A few months later, a NSA lawyer revealed during a Privacy and Civil Liberties Oversight Board meeting that [tech companies *did* know about the NSA collecting user data](http://www.bustle.com/articles/18740-nsa-says-tech-companies-knew-about-prism-aided-in-its-operation), and even helped them do the dirty deed. Now, Al Jazeera had got its hand on email communications between Google executives Eric Schmidt and Sergey Brin, and NSA Director Gen. Keith Alexander — which apparently reveals a much more cooperative relationship between large technology companies and our government than [we’ve been led to believe](http://www.reuters.com/article/2013/07/03/us-usa-security-siliconvalley-idUSBRE96214I20130703).

The emails, between Alexander and the Google executives, were exchanged one year before the Snowden revelations. Alexander extended an invitation to Schmidt in an email sent in June of 2012 for a “classified threat briefing” in August in California, which would “focus on Mobility Threats and Security.” In the same email, Alexander wrote about a previous meeting held with other industry leaders, and how he wanted Schmidt to attend an August meeting with “a small group of CEOs” to discuss “the security of mobility devices,” as well as the “specific threats,” as Al Jazeera reports.

It seems this small group made up the [Enduring Security Framework, a confidential government initiative](http://america.aljazeera.com/articles/2014/5/6/nsa-chief-google.html) that was launched in 2009 by 18 CEOs of U.S. companies, as well as deputy secretaries for the Department of Homeland Security and Defense. [ESF is meant to “coordinate government/industry actions](http://www.businessinsider.com/google-nsa-emails-2014-5#%21JMPgL) on important, generally classified security issues that couldn’t be solved by individual actors alone.” Some of the companies include Advanced Micro Devices, Dell, Hewlett-Packard, Intel, and Microsoft.

**May 7**

[Researchers find post-Snowden chill stifling our search terms](http://nakedsecurity.sophos.com/2014/05/08/researchers-find-post-snowden-chill-stifling-our-search-terms/)

[Anti-spying bill wins first round in Congress](http://rt.com/usa/157612-nsa-snowden-bill-congress/)

[The big business of data collection](http://onpoint.wbur.org/2014/05/07/big-data-nsa-data-collection-privacy)

**May 6**

[House to advance bill to end mass surveillance](http://www.nationaljournal.com/tech/house-to-advance-bill-to-end-mass-nsa-surveillance-20140505)

[Dueling NSA reform bills set for House](http://rt.com/usa/156976-nsa-reform-bill-house/)

[Almost no one opposes mass surveillance](http://www.theatlantic.com/politics/archive/2014/05/false-equivalence-on-surveillance-from-alan-dershowitz/361694/)

[Privacy alliance calls for internet reset](http://www.computerweekly.com/news/2240220119/Privacy-alliance-calls-for-internet-reset)

[Push back on privacy](http://fullcomment.nationalpost.com/2014/05/06/david-young-push-back-on-privacy/)

**May 5**

[Russia still stonewalling](http://www.courthousenews.com/2014/05/05/67579.htm)

[Michael Hayden’s unwitting case against surveillance](http://www.theatlantic.com/politics/archive/2014/05/michael-haydens-unwitting-case-against-secret-surveillance/361689/)

[Privacy more than about compliance, it’s vital to the economy](http://www.arnnet.com.au/article/544320/cebit_2014_privacy_about_more_than_compliance_its_vital_economy_ccu/)

[From NSA to race, a protector of rights needed](http://www.bostonglobe.com/opinion/2014/05/04/from-nsa-race-protector-rights-needed/nFG2cqKznWRCZGddVsJAoJ/story.html)

**May 4**

[Obama, Merkel struggle over spying, agree on trade](http://www.brecorder.com/business-a-economy/189/1179450/)

[All NSA intel goes directly to Israel](http://www.presstv.ir/detail/2014/05/04/361217/all-nsa-intel-goes-directly-to-israel/)

**May 3**

[](http://bauscharddebate.com/wp-content/uploads/2014/04/8863deaf-70ed-48b3-af3f-38c31d7ce32d_170x256-1.jpg)[Greenwald debates Hayden on surveillance](http://rt.com/usa/156536-hayden-greenwald-state-surveillance-debate/)

[8 thought-provoking quotes from the debate](http://mashable.com/2014/05/02/greenwald-nsa-debate/)

[Snowden: Everyone under surveillance now](http://www.delhidailynews.com/news/Everyone-under-surveillance-now--Snowden-1399111584/)

[US, Germany fail to reach an agreement to limit surveillance](http://www.stripes.com/news/us-germany-fail-to-reach-agreement-to-limit-surveillance-1.281304)

**May 2**

[The shaky legal foundations of NSA surveillance](http://www.theatlantic.com/politics/archive/2014/05/the-shaky-legal-foundation-of-nsa-surveillance-on-americans/361476/)

[US surveillance court hasn’t turned down an NSA request this decade](http://motherboard.vice.com/read/the-us-surveillance-court-hasnt-turned-down-an-nsa-request-this-decade)

[White House seeks legal immunity for firms that hand over customer data](http://www.theguardian.com/world/2014/may/02/white-house-legal-immunity-telecoms-firms-bill)

[Apple, Facebook, others notify users of secret data demands](http://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html)

[Is state surveillance a legitimate defense of our freedoms?](http://www.theglobeandmail.com/globe-debate/is-state-surveillance-a-legitimate-defence-of-our-freedoms/article18368244/)

[White House weighs in on online privacy](http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/01/the-white-house-finally-notices-online-privacy-rules-are-decades-out-of-date/)

[Merkel makes first visit since NSA scandal](http://www.dailysabah.com/europe/2014/05/02/merkel-makes-first-us-visit-since-nsa-scandal)

[In surveillance debate, White House turns its attention to Silicon Valley](http://www.nytimes.com/2014/05/03/us/politics/white-house-shifts-surveillance-debate-to-private-sector.html?_r=1)

David Sanger, New York Times, May 3, 2014http://www.nytimes.com/2014/05/03/us/politics/white-house-shifts-surveillance-debate-to-private-sector.html?\_r=1 “In Sureveillance Debate, White House turns to Sillicon Valley,” http://www.nytimes.com/2014/05/03/us/politics/white-house-shifts-surveillance-debate-to-private-sector.html?\_r=1

But by January, Mr. Obama had arrived in a different place. After approving, for five years, a government program to collect telephone metadata — the information about telephone numbers dialed and the duration of calls — he acceded to recommendations to leave that information in the hands of telecommunications companies. Quietly, the White House ended the wiretapping of dozens of foreign leaders.

**May 1**

[White House releases big data and privacy report](http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/01/white-house-releases-big-data-and-privacy-report/)

[The race to bring NSA surveillance to the Supreme Court](http://www.theverge.com/2014/5/1/5671532/will-nsa-surveillance-ever-get-to-the-supreme-court)

[GCHQ sought access to NSA surveillance data](http://www.scmagazine.com/gchq-sought-nsas-mass-collection-of-surveillance-data/article/345180/)

**April 30th**

[What we know about the NSA surveillance program](http://www.politifact.com/punditfact/article/2014/apr/30/what-we-know-about-nsa-surveillance-program/)

[US government reviews online privacy protection](http://www.itweb.co.za/index.php?option=com_content&view=article&id=134156:US-govt-reviews-online-privacy-protection&catid=845)

[How the NSA undermined one of Obama’s top priorities](http://www.nationaljournal.com/daily/how-the-nsa-undermined-one-of-obama-s-top-priorities-20140429)

[States adopt new rules on eavesdropping](http://www.landlinemag.com/Story.aspx?StoryID=26948)

**April 29th**

[White house explains ‘disciplined, rigorous’ NSA policy](http://thehill.com/policy/technology/204668-white-house-explains-disciplined-rigorous-nsa-policy)

**April 26**

[Surveillance Court rejected Verizon lawsuit](http://www.washingtonpost.com/world/national-security/surveillance-court-rejected-verizon-challenge-to-nsa-calls-program/2014/04/25/78d430c2-ccc2-11e3-93eb-6c0037dde2ad_story.html)

[NSA internal documents lay down surveillance practices](http://www.asiantribune.com/node/79305)

D[rone debate: Proposal sparks privacy concerns](http://wpri.com/2014/04/25/drone-proposal-draws-privacy-concerns-may14/)

[Privacy backers looking for email protections](http://thehill.com/policy/technology/204432-privacy-backers-looking-for-email-protections)

**April 25**

[Putin callas internet a CIA Project](http://horseedmedia.net/news/2014/04/putin-calls-internet-cia-project-renewing-fears-web-breakup/)

[Is the NSA reading your emails?](http://blog.nj.com/njv_donald_scarinci/2014/04/is_the_nsa_reading_your_emails.html)

[The rise of the American corporate security state](http://www.whistleblower.org/blog/04242014-essential-reading-rise-american-corporate-security-state)

[US defends intelligence sweep](http://www.ndtv.com/article/world/us-defends-intelligence-sweep-as-same-as-allies-386435?curl=1398357769)

**April 24**

[House members push for debate on NSA snooping](http://blogs.rollcall.com/218/house-members-push-for-open-debate-on-nsa-snooping/?dcz=)

[Face recognition is the end of anonymity](http://www.independent.co.uk/life-style/gadgets-and-tech/features/facerecognition-software-is-this-the-end-of-anonymity-for-all-of-us-9278697.html)

**April 23**

[Here’s who should watch the watchmen](http://www.thedailybeast.com/articles/2014/04/23/here-s-who-should-watch-the-watchmen.html)

[Despite fears, MSN, others bet on US data centers](http://channelnomics.com/2014/04/23/despite-nsa-fears-microsoft-others-bet-u-s-data-centers/)

[Brazil passes trailblazing internet privacy law](http://www.ticotimes.net/2014/04/23/brazil-passes-trailblazing-internet-privacy-law)

**April 22**

[How the Russian surveillance state works](http://boingboing.net/2014/04/22/how-the-russian-surveillance-s.html)

[NSA reveals how PRISM works, but nothing is new](http://mashable.com/2014/04/22/nsa-prism-report/)

[Google working on end to end encryption for Gmail](http://timesofindia.indiatimes.com/Tech/Tech-News/Google-working-on-end-to-end-encryption-in-Gmail-Report/articleshow/34077467.cms)

**April 21**

[Putin must be called to account on surveillance](http://www.towardfreedom.com/51-global-news-and-analysis/global-news-and-analysis/3512-putin-must-be-called-to-account-on-surveillance-just-like-obama)  
[Secret exceptions to reasonable suspicion: who watches those watching you?](http://blogs.computerworld.com/privacy/23812/secret-exceptions-reasonable-suspicion-who-watches-watchers-watching-you)

[The menace of secret government](http://reason.com/archives/2014/04/21/the-menace-of-secret-governmen)

[Americans don’t want drones at home](http://invests.com/americans-dont-want-drones-at-home-heres-why/20140421351115507)

**April 20**

[Snowden reporter promises more NSA revelations](https://thehill.com/blogs/hillicon-valley/technology/203936-snowden-reporter-promises-more-nsa-revelations)

[Freedom vs. security](http://blog.timesunion.com/opinion/freedom-versus-security/28705/)  
**April 19**

[Is data hoarding necessary for lawful surveillance?](http://www.huffingtonpost.com/joan-feigenbaum/data-hoarding-surveillance_b_5179305.html)

[As we sweat government surveillance, companies like Google collect data](http://www.theguardian.com/commentisfree/2014/apr/18/corporations-google-should-not-sell-customer-data)

**April 18**

[Does Russia spy on millions?](http://www.pri.org/stories/2014-04-18/does-russia-spy-communications-millions-individuals)  
[Supreme Court justices says they are likely to rule on surveillance](http://techcrunch.com/2014/04/18/supreme-court-justices-say-theyre-likely-to-rule-on-nsa-surveillance/)

**April 17**

[Ginsburg, Scalia discuss NSA freedoms](http://www.politico.com/story/2014/04/supreme-court-ruth-bader-ginsburg-antonin-scalia-105807.html)

**April 16th**

[NSA has piggy-backed on corporate surveillance programs](http://vr-zone.com/articles/nsa-piggybacked-corporate-surveillance-efforts-says-security-expert/75829.html)

[Civil society must act against unlawful surveillance of the internet](http://www.eurasiareview.com/15042014-civil-society-must-act-against-unlawful-surveillance-of-internet-users-oped/)

[Obama: NSA must reveal bugs like heartbleed](http://www.wired.com/2014/04/obama-zero-day/)

**April 15th**

[NSA surveillance program reaches into past](http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html)

[Two reporters who probed NSA surveillance back in US](http://www.washingtonpost.com/national/2-reporters-who-probed-nsa-surveillance-back-in-us/2014/04/11/fa0dcd6c-c199-11e3-9ee7-02c1e10a03f0_story.html)

[Are Google and Facebook just pretending they want limits on surveillance?](http://www.huffingtonpost.com/2014/04/11/google-facebook-nsa_n_5135834.html)

[New York police end Muslim surveillance program](http://www.usatoday.com/story/news/nation/2014/04/15/nypd-muslim-surveillance/7758229/)

**April 14th**

[Google knew about heartbleed and didn’t tell the government](http://www.nextgov.com/cio-briefing/2014/04/google-knew-about-heartbleed-and-didnt-tell-government/82528/)

**April 13th**

[Time to reign in the NSA surveillance state](https://www.aclu.org/time-rein-surveillance-state-0)

**April 12th**

[Silicon Valley could force NSA reform](http://www.theguardian.com/commentisfree/2014/apr/12/silicon-valley-nsa-reform-taking-so-long)

[NSA denies exploiting heartbleed bug](http://tech.firstpost.com/news-analysis/nsa-denies-having-exploited-heartbleed-bug-for-surveillance-purposes-221654.html)

**April 11th**

[Report says NSA exploited heartbleed bug](http://www.cnet.com/news/nsa-denies-it-knew-of-exploited-heartbleed-kept-flaw-secret/)

**April 10th**

[Merkel denied access to her NSA file](http://www.theguardian.com/world/2014/apr/10/angela-merkel-denied-access-nsa-file)

**April 9th**

[Lawmakers push US attorney general for surveillance changes](http://www.pcworld.com/article/2141260/lawmakers-push-us-attorney-general-for-nsa-surveillance-changes.html)

[Stop comparing NSA to 1984](http://www.theatlantic.com/entertainment/archive/2014/04/stop-comparing-the-nsa-to-em-1984-em-and-start-comparing-it-to-philip-k-dick/360353/)

[Internet governance body trying to stop NSA](http://rt.com/usa/wikileaks-netmundial-internet-governance-221/)

**April 8th**

[US Supreme Court passes on surveillance case](http://www.cnet.com/news/us-supreme-court-wont-look-at-nsa-bulk-phone-collection-practices/)

[Watch this debate on NSA surveillance](https://technical.ly/baltimore/2014/04/08/watch-debate-nsa-surveillance-hosted-johns-hopkins-video/)

**April 7th**

[Pay no attention to what they tell you, they are listening in](http://www.huffingtonpost.com/tom-engelhardt/pay-no-attention-to-what-_b_5105951.html)

**April 6th**

[Metadata monitoring more intrusive than eavesdropping](http://rt.com/news/snowden-greenwald-metadata-amnesty-757/)

[Snowden, Greenwald caution against wider government monitoring](http://www.huffingtonpost.com/2014/04/06/edward-snowden-glenn-greenwald_n_5098494.html)

**April 5th**

[NSA spying affecting online commerce](http://www.zdnet.com/new-harris-poll-finds-nsa-spying-affecting-online-commerce-7000028061/)

**April 4th**

[Can better encryption stop the NSA?](http://www.digitaltrends.com/opinion/can-better-encryption-yahoo-others-stop-nsa/)

**April 3rd**

[DOJ apologizes in NSA case](http://www.usnews.com/news/articles/2014/04/03/department-of-justice-apologizes-twice-to-court-in-nsa-case)

**April 2nd**

[NSA spying affecting online commerce](http://www.zdnet.com/new-harris-poll-finds-nsa-spying-affecting-online-commerce-7000028061/)

**April 1st**  
[White House pushes Congress to pass changes to NSA surveillance programs](http://www.washingtonpost.com/world/national-security/white-house-pushes-congress-to-quickly-pass-changes-to-nsa-surveillance-program/2014/03/27/1a2c4052-b5b9-11e3-8cb6-284052554d74_story.html)

[NSA performed warrantless searches on Americans calls](http://www.theguardian.com/world/2014/apr/01/nsa-surveillance-loophole-americans-data)

## Bibliography – Law Reviews on Privacy

1. © 2013 AHLA, Journal of Health & Life Sciences Law, Vol. 7, No. 1, Pg. 79, NOTE AND COMMENT: The Need for Privacy-Centric Role-Based Access Controls to Electronic Health Records

**October,** 2013

2. © 2011 AHLA, Journal of Health & Life Sciences Law, Vol. 5, No. 1, Pg. 75, PRACTICE RESOURCE: Genetic Privacy Laws: 50 State Survey

**October,** 2011

3. © 2011 AHLA, Journal of Health & Life Sciences Law, Vol. 4, No. 2, Pg. 173, PRACTICE RESOURCE: Data Privacy Concerns for U.S. Healthcare Enterprises' Overseas Ventures

**February,** 2011

4. Copyright (c) 2013 Air Force Judge Advocate General School The Air Force Law Review, 2013, Air Force Law Review, 70 A.F. L. Rev. 1, 12640 words, ARTICLE: PROTECTING SECURITY AND PRIVACY: AN ANALYTICAL FRAMEWORK FOR AIRBORNE DOMESTIC IMAGERY, COLONEL DAWN M.K. ZOLDI \*

5. Copyright (c) 2010 Akron Law Review Akron Law Review, 2010, Akron Law Review, 43 Akron L. Rev. 331, 47833 words, ARTICLE: CARPE DIEM: PRIVACY PROTECTION IN EMPLOYMENT ACT, Ariana R. Levinson \*

6. Copyright (c) 2013 University of Alabama Alabama Law Review, 2013, Alabama Law Review, 64 Ala. L. Rev. 845, 10510 words, ARTICLE: AN ETHICAL DUTY TO PROTECT ONE'S OWN INFORMATION PRIVACY?, Anita L. Allen \*

7. Copyright (c) 2012 Alaska Law Review Alaska Law Review, December, 2012, Alaska Law Review, 29 Alaska L. Rev. 175, 25049 words, ARTICLE: THE CONTINUING VITALITY OF RAVIN V. STATE: ALASKANS STILL HAVE A CONSTITUTIONAL RIGHT TO POSSESS MARIJUANA IN THE PRIVACY OF THEIR HOMES, Jason Brandeis\*

8. Copyright (c) 2014 Albany Law School Albany Government Law Review, 2014, Albany Government Law Review, 7 Alb. Gov't L. Rev. 591, 9694 words, NOTE: THE INTERNET AND SOCIAL MEDIA SITES: A SHIFT IN PRIVACY NORMS RESULTING IN THE EXPLOITATION AND ABUSE OF ADOLESCENTS AND TEENS IN DATING RELATIONSHIPS, Lauren McCormick\*

9. Copyright (c) 2014 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2014, Albany Law Journal of Science and Technology, 24 Alb. L.J. Sci. & Tech. 47, 14229 words, ARTICLE: KATZ ON A HOT TIN ROOF: THE REASONABLE EXPECTATION OF PRIVACY DOCTRINE IS RUDDERLESS IN THE DIGITAL AGE, UNLESS CONGRESS CONTINUALLY RESETS THE PRIVACY BAR, Charles E. MacLean\*

10. Copyright (c) 2014 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2014, Albany Law Journal of Science and Technology, 24 Alb. L.J. Sci. & Tech. 105, 44569 words, ARTICLE: IF PERSONAL INFORMATION IS PRIVACY'S GATEKEEPER, THEN RISK OF HARM IS THE KEY: A PROPOSED METHOD FOR DETERMINING WHAT COUNTS AS PERSONAL INFORMATION, Eloise Gratton\*

11. Copyright (c) 2013 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2013, Albany Law Journal of Science and Technology, 23 Alb. L.J. Sci. & Tech. 55, 11616 words, ARTICLE: SHARING YOU WITH YOU: INFORMATIONAL PRIVACY, GOOGLE, & THE LIMITS OF USE LIMITATION, Kevin P. McLaughlin\*

12. Copyright (c) 2011 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2011, Albany Law Journal of Science and Technology, 21 Alb. L.J. Sci. & Tech. 61, 28846 words, ARTICLE: PERSONAL JURISDICTION, INTERNET COMMERCE, AND PRIVACY: THE PERVASIVE LEGAL CONSEQUENCES OF MODERN GEOLOCATION TECHNOLOGIES, Kevin F. King\*

13. Copyright (c) 2011 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2011, Albany Law Journal of Science and Technology, 21 Alb. L.J. Sci. & Tech. 591, 19325 words, COMMENT: INVASION CONTRACTS: THE PRIVACY IMPLICATIONS OF TERMS OF USE AGREEMENTS IN THE ONLINE SOCIAL MEDIA SETTING, Jared S. Livingston

14. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, ALBANY LAW JOURNAL OF SCIENCE & TECHNOLOGY, 20 Alb. L.J. Sci. & Tech. 203, 13321 words, COMMENT: PRIVACY AND SECURITY OF PERSONAL HEALTH RECORDS MAINTAINED BY ONLINE HEALTH SERVICES, Jenna Caldarella

15. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, Albany Law Journal of Science & Technology, 20 Alb. L.J. Sci. & Tech. 247, 36240 words, Symposium Issue: e-Legal: Privacy and Law Enforcement on the World Wide Web: ARTICLE: WIKIPEDIA: A REPUBLIC OF SCIENCE DEMOCRATIZED, Shun-Ling Chen\*

16. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, Albany Law Journal of Science & Technology, 20 Alb. L.J. Sci. & Tech. 327, 15393 words, Symposium Issue: e-Legal: Privacy and Law Enforcement on the World Wide Web: ARTICLE: BALANCING ANONYMITY, POPULARITY, & MICRO-CELEBRITY: THE CROSSROADS OF SOCIAL NETWORKING & PRIVACY, Brian Kane

17. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, Albany Law Journal of Science & Technology, 20 Alb. L.J. Sci. & Tech. 365, 3705 words, Symposium Issue: e-Legal: Privacy and Law Enforcement on the World Wide Web: PRESENTATION: CLOUD COMPUTING: PRIVACY STORM ON THE HORIZON?, Andrew C. DeVore

18. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, Albany Law Journal of Science & Technology, 20 Alb. L.J. Sci. & Tech. 375, 3552 words, Symposium Issue: e-Legal: Privacy and Law Enforcement on the World Wide Web: PRESENTATION: RETHINKING THE INTERNET'S PRIVACY DILEMMA: A MODEST CALL FOR INFORMED, NIMBLE SOLUTIONS, Brian Kane

19. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, Albany Law Journal of Science & Technology, 20 Alb. L.J. Sci. & Tech. 385, 2618 words, Symposium Issue: e-Legal: Privacy and Law Enforcement on the World Wide Web: PRESENTATION: NATIONAL INFORMATION INSECURITY: RECENT INITIATIVES IN PRIVATE SECTOR INFORMATION SECURITY, John Kennedy

20. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, Albany Law Journal of Science & Technology, 20 Alb. L.J. Sci. & Tech. 393, 1800 words, Symposium Issue: e-Legal: Privacy and Law Enforcement on the World Wide Web: PRESENTATION: SELF REGULATION OR PRIVACY LEGISLATION, Dale Skivington - Former Chief Privacy Officer, Eastman Kodak

21. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, Albany Law Journal of Science & Technology, 20 Alb. L.J. Sci. & Tech. 399, 3121 words, Symposium Issue: e-Legal: Privacy and Law Enforcement on the World Wide Web: PRESENTATION: NEW YORK STATE INFORMATION SECURITY BREACH AND NOTIFICATION ACT: STATE BREACH NOTIFICATION REQUIREMENTS, Thomas Smith

22. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, Albany Law Journal of Science & Technology, 20 Alb. L.J. Sci. & Tech. 407, 5078 words, Symposium Issue: e-Legal: Privacy and Law Enforcement on the World Wide Web: PRESENTATION: THE CLASH OF TITANIC PARADIGMS - THE AMERICAN CRIMINAL JUSTICE SYSTEM VERSUS MODERN COMPUTER TECHNOLOGY: THE GREATEST UNRESOLVEABLE CONFLICT BETWEEN A SQUARE PEG AND ROUND HOLE?, Stephen Treglia

23. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, Albany Law Journal of Science & Technology, 20 Alb. L.J. Sci. & Tech. 421, 4364 words, Symposium Issue: e-Legal: Privacy and Law Enforcement on the World Wide Web: PRESENTATION: SELF-GOVERNING ONLINE COMMUNITIES IN WEB 2.0: PRIVACY, ANONYMITY AND ACCOUNTABILITY IN WIKIPEDIA, Shun-Ling Chen

24. Copyright (c) 2010 Albany Law Journal of Science & Technology Albany Law Journal of Science & Technology, 2010, Albany Law Journal of Science & Technology, 20 Alb. L.J. Sci. & Tech. 487, 19470 words, ARTICLE: BIT-WISE BUT PRIVACY FOOLISH: SMARTER E-MESSAGING TECHNOLOGIES CALL FOR A RETURN TO CORE PRIVACY PRINCIPLES, John Soma, Melodi Mosley Gates, & Michael Smith\*

25. Copyright (c) 2013 The Harvard Law Review Association Harvard Law Review Forum, May, 2013, Harvard Law Review Forum, 126 Harv. L. Rev. F. 241, 5383 words, PRIVACY LAW: POSITIVE THEORY AND NORMATIVE PRACTICE, Anita L. Allen

26. Copyright (c) 2010 The Harvard Law Review Association Harvard Law Review Forum, December, 2010, Harvard Law Review Forum, 124 Harv. L. Rev. F. 656, 207 words, RECENT PUBLICATION: BECAUSE IT IS WRONG: TORTURE, PRIVACY, AND PRESIDENTIAL POWER IN THE AGE OF TERROR.

27. Copyright (c) 2011 Albany Law School Albany Law Review, 2011 / 2012, Albany Law Review, 75 Alb. L. Rev. 341, 18188 words, COMMENT: REGULATING THE USE AND SHARING OF ENERGY CONSUMPTION DATA: ASSESSING CALIFORNIA'S SB 1476 SMART METER PRIVACY STATUTE, John R. Forbush\*

28. American Bankruptcy Institute, 33-4 ABIJ 16, April 2014, Affairs of State I:, By Nicole D. Mignone n1, 2639 words

**Privacy** Protection for Dating-Website Customers

29. American Bankruptcy Institute Journal, 31-10 ABIJ 28, November 2012, News at 11, By Kenneth M. Misken and Camisha L. Simmons n1, 2912 words

Government Addresses **Privacy** Concerns in Bankruptcy Sales

30. American Bankruptcy Institute, 29-8 ABIJ 38, October 2010, Feature, Written by: Warren E. Agin, Swiggart & Agin LLC; Boston, wea@swiggartagin.com, 3635 words

Reconciling the FTC Act with the Consumer **Privacy** Ombudsman's Role

31. American Bankruptcy Institute, 29-7 ABIJ 36, September 2010, Column, Privacy Rights and PACER: Keeping Your Clients' Privacy Secure, Contributing Editor: Timothy B. McGrath, US Bankruptcy Court (ED, Pa.); Philadelphia, timothy\_mcgrath@paeb.uscourts.gov, 1319 words

32. Copyright (c) 2013 Academy of Legal Studies in Business American Business Law Journal, Summer, 2013, American Business Law Journal, 50 Am. Bus. L.J. 413, 28175 words, ARTICLE: What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data, Nancy J. King \* and V.T. Raja \*\*

33. Copyright (c) 2012 Academy of Legal Studies in Business American Business Law Journal, Spring, 2012, American Business Law Journal, 49 Am. Bus. L.J. 63, 25265 words, ARTICLE: Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee, Patricia Sánchez Abril, \* Avner Levin, \*\* and Alissa Del Riego \*\*\*

34. Copyright (c) 2012 Academy of Legal Studies in Business American Business Law Journal, Spring, 2012, American Business Law Journal, 49 Am. Bus. L.J. 125, 40792 words, ARTICLE: Fragile Merchandise: A Comparative Analysis of the Privacy Rights for Public Figures, Scott. J. Shackelford \*

35. Copyright (c) 2011 Academy of Legal Studies in Business American Business Law Journal, Fall, 2011, American Business Law Journal, 48 Am. Bus. L.J. 503, 43104 words, ARTICLE: A Proposed National Health Information Network Architecture and Complementary Federal Preemption of State Health Information Privacy Laws, John W. Hill, \* Arlen W. Langvardt, \*\* Anne P. Massey, \*\*\* and Jonathan E. Rinehart \*\*\*\*

36. Copyright (c) 2012 American Criminal Law Review American Criminal Law Review, Fall, 2012, American Criminal Law Review, 49 Am. Crim. L. Rev. 1777, 21998 words, ARTICLE: IT'S COMPLICATED: PRIVACY AND DOMESTIC VIOLENCE, Kimberly D. Bailey \*

37. Copyright (c) 2010 American Indian Law Review American Indian Law Review, 2010 / 2011, American Indian Law Review, 35 Am. Indian L. Rev. 729, 20883 words, COMMENT: SELF-INTERESTED: PROTECTING THE CULTURAL AND RELIGIOUS PRIVACY OF NATIVE AMERICANS THROUGH THE PROMOTION OF PROPERTY RIGHTS IN BIOLOGICAL MATERIALS, Kimberly Self\*

38. Copyright (c) 2011 The American Society of Comparative Law, Inc. The American Journal of Comparative Law, Spring, 2011, The American Journal of Comparative Law, 59 Am. J. Comp. L. 411, 23503 words, ARTICLE: Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy+, FRANCESCA BIGNAMI\*

39. Copyright (c) 2011 The University of Texas School of Law American Journal of Criminal Law, Summer, 2011, American Journal of Criminal Law, 38 Am. J. Crim. L. 289, 42685 words, Article: Quantifying Katz: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context, Henry F. Fradella\*, Weston J. Morrow\*\*, Ryan G. Fischer\*\*\*, and Connie Ireland\*\*\*\*

40. Copyright (c) 2012 American Society of Law, Medicine & Ethics, Inc., and Boston University American Journal of Law & Medicine, 2012, American Journal of Law & Medicine, 38 Am. J. L. and Med. 225, 2128 words, NOTE AND RECENT CASE DEVELOPMENT: Recent Case Developments, Shuyuan Hu

Minnesota Supreme Court Hears Whether the Genetic **Privacy** Act Protects Newborn Blood Spot Samples Obtained ...

41. Copyright (c) 2010 American Society of Law, Medicine & Ethics, Inc., and Boston University American Journal of Law & Medicine, 2010, American Journal of Law & Medicine, 36 Am. J. L. and Med. 586, 17412 words, ARTICLE: Patient Data: Property, Privacy & the Public Interest, Marc A. Rodwin, J.D., Ph.D. +

42. Copyright (c) 2012 American University Journal of Gender, Social Policy & the Law American University Journal of Gender, Social Policy & the Law, 2012, American University Journal of Gender, Social Policy & the Law, 21 Am. U.J. Gender Soc. Pol'y & L. 481, 12351 words, COMMENT: PUBLIC HEALTH VS. PRIVACY: REBALANCING THE GOVERNMENT INTEREST IN INVOLUNTARY PARTNER-NOTIFICATION FOLLOWING ADVANCEMENTS IN HIV TREATMENT, Leah H. Wissow\*

43. Copyright (c) 2011 American University Journal of Gender, Social Policy & the Law American University Journal of Gender, Social Policy & the Law, 2011, American University Journal of Gender, Social Policy & the Law, 19 Am. U.J. Gender Soc. Pol'y & L. 1351, 11062 words, COMMENT: MOSAIC THEORY AND THE FOURTH AMENDMENT: HOW JONES CAN SAVE PRIVACY IN THE FACE OF EVOLVING TECHNOLOGY, Madelaine Virginia Ford\*

44. Copyright (c) 2012 Houston Journal of Health Law & Policy Houston Journal of Health Law & Policy, Symposium, 2012, Houston Journal of Health Law & Policy, 12 Hous. J. Health L. & Pol'y 171, 11789 words, HEALTH DATA SECURITY SYMPOSIUM: When Patients Interact with EHRs: Problems of Privacy and Confidentiality, Leslie P. Francis\*

45. Copyright (c) 2011 American University International Law Review American University International Law Review, 2011, American University International Law Review, 26 Am. U. Int'l L. Rev. 601, 17054 words, FOCUS ISSUE: INTELLECTUAL PROPERTY LAW ENFORCEMENT AND THE ANTI-COUNTERFEITING TRADE AGREEMENT (ACTA): ARTICLE: Enforcing Intellectual Property Rights by Diminishing Privacy: How the Anti-Counterfeiting Trade Agreement Jeopardizes the Right to Privacy, Alberto J. Cerda Silva\*

46. Copyright (c) 2011 State Bar of Texas, Litigation Section. All Rights Reserved. The Advocate, Fall, 2011, 56 The Advocate 60, 7491 words, SYMPOSIUM: COMMERCIAL LAW DEVELOPMENTS AND DOCTRINE: PART II. RECENT, LEADING DOCTRINAL DEVELOPMENTS: PRIVACY RIGHTS OF EMPLOYEES IN AN ELECTRONIC WORLD, BY MICHAEL KELSHEIMER & TRAVIS CRABTREE

47. Copyright (c) 2013 American University Law Review American University Law Review, June, 2013, American University Law Review, 62 Am. U.L. Rev. 1113, 7252 words, AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD: FOREWORD: MAPPING TODAY'S CYBERSECURITY LANDSCAPE, Jorge L. Contreras\*, Laura DeNardis\*\* and Melanie Teplinsky\*\*\*

48. Copyright (c) 2013 American University Law Review American University Law Review, June, 2013, American University Law Review, 62 Am. U.L. Rev. 1131, 5703 words, AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD: KEYNOTE TRANSCRIPT: LEAP-AHEAD PRIVACY AS A GOVERNMENT RESPONSIBILITY IN THE DIGITAL AGE, Ivan K. Fong\* and David G. Delaney\*\*

49. Copyright (c) 2013 American University Law Review American University Law Review, June, 2013, American University Law Review, 62 Am. U.L. Rev. 1145, 28168 words, AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD: ARTICLE: REGULATING INFORMATION SECURITY IN THE GOVERNMENT CONTRACTING INDUSTRY: WILL THE RISING TIDE LIFT ALL THE BOATS?, Keir X. Bancroft\*

50. Copyright (c) 2013 American University Law Review American University Law Review, June, 2013, American University Law Review, 62 Am. U.L. Rev. 1203, 17011 words, AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD: ARTICLE: WHEN CYBERWEAPONS END UP ON PRIVATE NETWORKS: THIRD AMENDMENT IMPLICATIONS FOR CYBERSECURITY POLICY, Alan Butler\*

51. Copyright (c) 2013 American University Law Review American University Law Review, June, 2013, American University Law Review, 62 Am. U.L. Rev. 1243, 12273 words, AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD: ARTICLE: HACKER'S DELIGHT: LAW FIRM RISK AND LIABILITY IN THE CYBER AGE, Michael McNerney\* and Emilian Papadopoulos\*\*

52. Copyright (c) 2013 American University Law Review American University Law Review, June, 2013, American University Law Review, 62 Am. U.L. Rev. 1273, 40572 words, AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD: ARTICLE: TOWARD CYBERPEACE: MANAGING CYBERATTACKS THROUGH POLYCENTRIC GOVERNANCE, Scott J. Shackelford\*

53. Copyright (c) 2013 American University Law Review American University Law Review, June, 2013, American University Law Review, 62 Am. U.L. Rev. 1365, 17386 words, AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD: COMMENT: IDENTITY CRISIS: SEEKING A UNIFIED APPROACH TO PLAINTIFF STANDING FOR DATA SECURITY BREACHES OF SENSITIVE PERSONAL INFORMATION, Miles L. Galbraith\*

54. Copyright (c) 2013 American University Law Review American University Law Review, June, 2013, American University Law Review, 62 Am. U.L. Rev. 1401, 6898 words, AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD: NOTE: FTC V. LABMD: FTC JURISDICTION OVER INFORMATION PRIVACY IS "PLAUSIBLE," BUT HOW FAR CAN IT GO?, Peter S. Frechette\*

55. Copyright (c) 2013 American University Law Review American University Law Review, June, 2013, American University Law Review, 62 Am. U.L. Rev. 1417, 9346 words, AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD: NOTE: REINING IN THE ROGUE EMPLOYEE: THE FOURTH CIRCUIT LIMITS EMPLOYEE LIABILITY UNDER THE CFAA, Danielle E. Sunberg\*

56. Copyright (c) 2011 American University Law Review American University Law Review, December, 2011, American University Law Review, 61 Am. U.L. Rev. 279, 25082 words, ARTICLE: FUNERAL PROTESTS, PRIVACY, AND THE CONSTITUTION: WHAT IS NEXT AFTER PHELPS?, Mark Strasser\*

57. Copyright (c) 2012 Loyola University Chicago School of Law, Beazley Institute for Health Law and Policy Annals of Health Law, Winter, 2012, Annals of Health Law, 21 Ann. Health L. 447, 26576 words, ARTICLE: Prescription Data Mining, Medical Privacy and the First Amendment: The U.S. Supreme Court in Sorrell v. IMS Health Inc., Marcia M. Boumil\*, Kaitlyn Dunn\*\*, Nancy Ryan,\*\*\* and Katrina Clearwater\*\*\*\*

58. Copyright (c) 2012 Appeal Publishing Society, Unviersity of Victoria, Faculty of Law, Canada Appeal: Review of Current Law and Law Reform, 2012, Appeal: Review of Current Law and Law Reform, 17 Appeal 63, 13974 words, ARTICLE: OUR DIGITAL SELVES: PRIVACY ISSUES IN ONLINE BEHAVIOURAL ADVERTISING, By Christopher Scott \*

59. Copyright (c) 2011 Arizona Board of Regents Arizona Journal of International and Comparative Law, Symposium, 2011, Arizona Journal of International and Comparative Law, 28 Ariz. J. Int'l & Comp. Law 501, 22961 words, NOTE: PROGRESS, PRIVACY, AND PREEMPTION: A STUDY OF THE REGULATORY HISTORY OF STORED-VALUE CARDS IN THE UNITED STATES AND THE EUROPEAN UNION, Naomi Claxton\*

60. Copyright (c) 2013 Arizona Board of Regents Arizona Law Review, 2013, Arizona Law Review, 55 Ariz. L. Rev. 997, 10598 words, ARTICLE: PRIVACY PROTESTS: SURVEILLANCE EVASION AND FOURTH AMENDMENT SUSPICION, Elizabeth E. Joh \*

61. Copyright (c) 2013 Arizona Board of Regents Arizona Law Review, 2013, Arizona Law Review, 55 Ariz. L. Rev. 1171, 10419 words, ARTICLE: OF INFORMATION, TRUST, AND ICE CREAM: A RECIPE FOR A DIFFERENT PERSPECTIVE ON THE PRIVACY OF HEALTH INFORMATION, Jana Sutton \*

62. Copyright (c) 2011 Arizona Board of Regents Arizona Law Review, Fall, 2011, Arizona Law Review, 53 Ariz. L. Rev. 985, 15805 words, NOTE: Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches, Corey J. Mantei\*

63. Copyright (c) 2013 Arizona State Law Journal Arizona State Law Journal, Fall, 2013, Arizona State Law Journal, 45 Ariz. St. L.J. 1277, 11095 words, COMMENT: Privacy in the Age of Smartphones: A Better Standard for GPS Tracking, Andrew McNichol\*

64. Copyright (c) 2013 Board of Trustees of the University of Arkansas University of Arkansas at Little Rock Law Review, Spring, 2013, University of Arkansas at Little Rock Law Review, 35 U. Ark. Little Rock L. Rev. 439, 50587 words, ARTICLE: THE RIGHT OF PRIVACY IN ARKANSAS: A PROGRESSIVE STATE, J. Lyn Entrikin\*

65. Copyright (c) 2012 Board of Trustees of the University of Arkansas University of Arkansas at Little Rock Law Review, Summer, 2012, University of Arkansas at Little Rock Law Review, 34 U. Ark. Little Rock L. Rev. 689, 12413 words, ARTICLE: PRIVACY FOR SOCIAL NETWORKING, Connie Davis Powell\*

66. Copyright (c) 2012 Board of Trustees of the University of Arkansas University of Arkansas at Little Rock Law Review, Summer, 2012, University of Arkansas at Little Rock Law Review, 34 U. Ark. Little Rock L. Rev. 747, 9621 words, ARTICLE: WALLED GARDENS OF PRIVACY OR "BINDING CORPORATE RULES?": A CRITICAL LOOK AT INTERNATIONAL PROTECTION OF ONLINE PRIVACY, Joanna Kulesza\*

67. Copyright (c) 2013 University of Baltimore School of Law The University of Baltimore Law Forum, Fall, 2013, University of Baltimore Law Forum, 44 U. Balt. L.F. 103, 1383 words, RECENT DEVELOPMENT: WALKER V. STATE: FOURTH AMENDMENT RIGHTS ARE NOT VIOLATED WHERE AN EMPLOYEE DOES NOT DEMONSTRATE A SUBJECTIVE EXPECTATION OF PRIVACY IN THE AREA SEARCHED; SEXUAL EXPLOITATION OF A CHILD CAN OCCUR WITHOUT ANY PHYSICAL CONTACT OR CRIMINAL INTENT., By Brittaney Fabiano

68. Copyright (c) 2014 The University of Baltimore Law Review University of Baltimore Law Review, Spring, 2014, University of Baltimore Law Review, 43 U. Balt. L. Rev. 199, 11552 words, COMMENT: WHAT'S YOURS IS OURS? GAMETE DONATION IN THE MARITAL CONTEXT: WHY COURTS AND LEGISLATURES SHOULD NOT INTERFERE WITH AN INDIVIDUAL'S FUNDAMENTAL RIGHT TO PRIVACY, Emily K. Alt\*

69. Copyright (c) 2013 The University of Baltimore Law Review University of Baltimore Law Review, Spring, 2013, University of Baltimore Law Review, 42 U. Balt. L. Rev. 391, 1429 words, PRIVACY RIGHTS & PROACTIVE INVESTIGATIONS: 2013 SYMPOSIUM ON EMERGING CONSTITUTIONAL ISSUES IN LAW ENFORCEMENT: FOREWORD: PRIVACY RIGHTS AND PROACTIVE INVESTIGATIONS: EMERGING CONSTITUTIONAL ISSUES IN LAW ENFORCEMENT, Thiru Vignarajah+

70. Copyright (c) 2013 The University of Baltimore Law Review University of Baltimore Law Review, Spring, 2013, University of Baltimore Law Review, 42 U. Balt. L. Rev. 395, 25229 words, PRIVACY RIGHTS & PROACTIVE INVESTIGATIONS: 2013 SYMPOSIUM ON EMERGING CONSTITUTIONAL ISSUES IN LAW ENFORCEMENT: ARTICLE: POST-JONES: HOW DISTRICT COURTS ARE ANSWERING THE MYRIAD QUESTIONS RAISED BY THE SUPREME COURT'S DECISION IN UNITED STATES V. JONES, Jason D. Medinger\*

71. Copyright (c) 2013 The University of Baltimore Law Review University of Baltimore Law Review, Spring, 2013, University of Baltimore Law Review, 42 U. Balt. L. Rev. 445, 17520 words, PRIVACY RIGHTS & PROACTIVE INVESTIGATIONS: 2013 SYMPOSIUM ON EMERGING CONSTITUTIONAL ISSUES IN LAW ENFORCEMENT: ARTICLE: BACK TO THE FUTURE: UNITED STATES V. JONES RESUSCITATES PROPERTY LAW CONCEPTS IN FOURTH AMENDMENT JURISPRUDENCE, Nancy Forster

72. Copyright (c) 2013 The University of Baltimore Law Review University of Baltimore Law Review, Spring, 2013, University of Baltimore Law Review, 42 U. Balt. L. Rev. 485, 14589 words, PRIVACY RIGHTS & PROACTIVE INVESTIGATIONS: 2013 SYMPOSIUM ON EMERGING CONSTITUTIONAL ISSUES IN LAW ENFORCEMENT: ARTICLE: LOCATION, LOCATION, LOCATION: BALANCING CRIME FIGHTING NEEDS AND PRIVACY RIGHTS, By Nancy K. Oliver\*

73. Copyright (c) 2013 The University of Baltimore Law Review University of Baltimore Law Review, Spring, 2013, University of Baltimore Law Review, 42 U. Balt. L. Rev. 513, 11599 words, PRIVACY RIGHTS & PROACTIVE INVESTIGATIONS: 2013 SYMPOSIUM ON EMERGING CONSTITUTIONAL ISSUES IN LAW ENFORCEMENT: ARTICLE: RESEARCH AND REALITY: BETTER UNDERSTANDING THE DEBATE BETWEEN SEQUENTIAL AND SIMULTANEOUS PHOTO ARRAYS, Frederick H. Bealefeld III\*

74. Copyright (c) 2013 The University of Baltimore Law Review University of Baltimore Law Review, Spring, 2013, University of Baltimore Law Review, 42 U. Balt. L. Rev. 535, 10730 words, PRIVACY RIGHTS & PROACTIVE INVESTIGATIONS: 2013 SYMPOSIUM ON EMERGING CONSTITUTIONAL ISSUES IN LAW ENFORCEMENT: ARTICLE: THE IMPERATIVE OF EYEWITNESS IDENTIFICATION REFORM AND THE ROLE OF POLICE LEADERSHIP, Rebecca Brown and Stephen Saloom\*

75. Copyright (c) 2013 The University of Baltimore Law Review University of Baltimore Law Review, Spring, 2013, University of Baltimore Law Review, 42 U. Balt. L. Rev. 561, 15193 words, PRIVACY RIGHTS & PROACTIVE INVESTIGATIONS: 2013 SYMPOSIUM ON EMERGING CONSTITUTIONAL ISSUES IN LAW ENFORCEMENT: ARTICLE: INDECENT EXPOSURE: GENES ARE MORE THAN A BRAND NAME LABEL IN THE DNA DATABASE DEBATE, By: Jessica D. Gabel\*

76. Copyright (c) 2013 The University of Baltimore Law Review University of Baltimore Law Review, Spring, 2013, University of Baltimore Law Review, 42 U. Balt. L. Rev. 591, 9605 words, PRIVACY RIGHTS & PROACTIVE INVESTIGATIONS: 2013 SYMPOSIUM ON EMERGING CONSTITUTIONAL ISSUES IN LAW ENFORCEMENT: ARTICLE: WHY DNA DATABASING IS GOOD FOR MARYLAND: A DNA ANALYST'S PERSPECTIVE, By Rana Santos\*

77. Copyright (c) 2012 The Regents of the University of California on behalf of Berkeley Journal of Gender, Law & Justice, Winter, 2012, Berkeley Journal of Gender, Law & Justice, 27 Berkeley J. Gender L. & Just. 28, 19863 words, ARTICLE: Reframing Roe: Property over Privacy\*, Rebecca L. Rausch+

78. Copyright (c) 2014 Regents of the University of California Berkeley Technology Law Journal, Spring, 2014, Berkeley Technology Law Journal, 29 Berkeley Tech. L.J. 61, 29904 words, ARTICLE: Why Not Privacy by Default?, Lauren E. Willis+

79. Copyright (c) 2013 Regents of the University of California Berkeley Technology Law Journal, Annual Review, 2013, Berkeley Technology Law Journal, 28 Berkeley Tech. L.J. 937, 13004 words, PRIVACY LAW: The Fourth Amendment and Government Interception of Unsecured Wireless Communications, Shaina Hyder+

80. Copyright (c) 2013 Regents of the University of California Berkeley Technology Law Journal, Annual Review, 2013, Berkeley Technology Law Journal, 28 Berkeley Tech. L.J. 963, 19035 words, PRIVACY LAW: Fraley v. Facebook: The Right of Publicity in Online Social Networks, Jesse Koehler+

81. Copyright (c) 2013 Regents of the University of California Berkeley Technology Law Journal, Annual Review, 2013, Berkeley Technology Law Journal, 28 Berkeley Tech. L.J. 1003, 16252 words, PRIVACY LAW: Jonesing for a Test: Fourth Amendment Privacy in the Wake of United States v. Jones, Lauren Elena Smith+

82. Copyright (c) 2013 Regents of the University of California Berkeley Technology Law Journal, Fall, 2013, Berkeley Technology Law Journal, 28 Berkeley Tech. L.J. 1333, 38683 words, ARTICLE: Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents, Ira S. Rubinstein+ and Nathaniel Good++

83. Copyright (c) 2012 Regents of the University of California Berkeley Technology Law Journal, Annual Review, 2012, Berkeley Technology Law Journal, 27 Berkeley Tech. L.J. 809, 16093 words, PRIVACY LAW: A Way Forward After Warshak: Fourth Amendment Protections for E-mail, Courtney M. Bowman+

84. Copyright (c) 2012 Regents of the University of California Berkeley Technology Law Journal, Annual Review, 2012, Berkeley Technology Law Journal, 27 Berkeley Tech. L.J. 837, 28033 words, PRIVACY LAW: Using Social Networking To Discuss Work: NLRB Protection for Derogatory Employee Speech and Concerted Activity, Ariana C. Green+

85. Copyright (c) 2011 Regents of the University of California Berkeley Technology Law Journal, Annual Review 2011, Berkeley Technology Law Journal, 26 Berkeley Tech. L.J. 773, 23058 words, PRIVACY LAW: A. NOTE: The Truth Can Catch the Lie: The Flawed Understanding of Online Speech in In re Anonymous Online Speakers, Musetta Durkee+

86. Copyright (c) 2011 Regents of the University of California Berkeley Technology Law Journal, Annual Review 2011, Berkeley Technology Law Journal, 26 Berkeley Tech. L.J. 823, 17882 words, PRIVACY LAW: A. NOTE: Locating Location Privacy, David H. Goetz+

87. Copyright (c) 2011 Regents of the University of California Berkeley Technology Law Journal, Annual Review 2011, Berkeley Technology Law Journal, 26 Berkeley Tech. L.J. 859, 24785 words, PRIVACY LAW: A. NOTE: Ontario v. Quon: In Search of A Reasonable Fourth Amendment, Miles K. Palley+

88. Copyright (c) 2011 Regents of the University of California Berkeley Technology Law Journal, Annual Review 2011, Berkeley Technology Law Journal, 26 Berkeley Tech. L.J. 905, 1531 words, PRIVACY LAW: B. ADDITIONAL DEVELOPMENTS - Privacy Law

89. Copyright (c) 2011 Regents of the University of California Berkeley Technology Law Journal, Spring, 2011, Berkeley Technology Law Journal, 26 Berkeley Tech. L.J. 979, 24066 words, ARTICLE: Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States, Lothar Determann+ and Robert Sprague++

90. Copyright (c) 2011 Regents of the University of California Berkeley Technology Law Journal, Symposium, 2011, Berkeley Technology Law Journal, 26 Berkeley Tech. L.J. 1409, 20358 words, SYMPOSIUM: TECHNOLOGY: TRANSFORMING THE REGULATORY ENDEAVOR: ARTICLE: Regulating Privacy by Design, Ira S. Rubinstein+

91. Copyright (c) 2010 Regents of the University of California Berkeley Technology Law Journal, Annual Review, 2010, Berkeley Technology Law Journal, 25 Berkeley Tech. L.J. 621, 14865 words, V. PRIVACY LAW: A. NOTES: Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless, David S. Barnhill

92. Copyright (c) 2010 Regents of the University of California Berkeley Technology Law Journal, Annual Review, 2010, Berkeley Technology Law Journal, 25 Berkeley Tech. L.J. 649, 12292 words, V. PRIVACY LAW: A. NOTES: IMS Health v. Ayotte: A New Direction on Commercial Speech Cases, Alexander D. Baxter

93. Copyright (c) 2010 Regents of the University of California Berkeley Technology Law Journal, Annual Review, 2010, Berkeley Technology Law Journal, 25 Berkeley Tech. L.J. 671, 15983 words, V. PRIVACY LAW: A. NOTES: The Death of the Privacy Policy?: Effective Privacy Disclosures After In re Sears, Yan Fang

94. Copyright (c) 2010 Regents of the University of California Berkeley Technology Law Journal, Annual Review, 2010, Berkeley Technology Law Journal, 25 Berkeley Tech. L.J. 701, 1850 words, V. PRIVACY LAW: B. Additional Developments

95. Copyright (c) 2010 Regents of the University of California Berkeley Technology Law Journal, Spring, 2010, Berkeley Technology Law Journal, 25 Berkeley Tech. L.J. 831, 36408 words, ARTICLE: Communications Privacy in the Military, Justin Holbrook+

96. Copyright (c) 2013 Boston College Law School Boston College International and Comparative Law Review, Spring, 2013, Boston College International and Comparative Law Review, 36 B.C. Int'l & Comp. L. Rev. 1455, 18987 words, NOTE: PRISONERS OF FAME: HOW AN EXPANDED USE OF INTRUSION UPON PSYCHOLOGICAL SECLUSION CAN PROTECT THE PRIVACY OF FORMER PUBLIC FIGURES, DAVID LIBARDONI \*

97. Copyright (c) 2011 Boston College Law School Boston College International and Comparative Law Review, Spring, 2011, Boston College International and Comparative Law Review, 34 B.C. Int'l & Comp. L. Rev. 477, 6240 words, COMMENT: THE INTERNET IS NOT A LAWLESS PRAIRIE: DATA PROTECTION AND PRIVACY IN ITALY, NOAH C.N. HAMPSON \*

98. Copyright (c) 2013 Boston College Law School Boston College Law Review, May, 2013, Boston College Law Review, 54 B.C. L. Rev 1455, 10250 words, ARTICLE: PRISONERS OF FAME: HOW AN EXPANDED USE OF INTRUSION UPON PSYCHOLOGICAL SECLUSION CAN PROTECT THE PRIVACY OF FORMER PUBLIC FIGURES, DAVID LIBARDONI \*

99. Copyright (c) 2013 Boston College Law School Boston College Law Review, March, 2013, Boston College Law Review, 54 B.C. L. Rev 789, 17465 words, NOTE: NO CILIA LEFT BEHIND: ANALYZING THE PRIVACY RIGHTS IN ROUTINELY SHED DNA FOUND AT CRIME SCENES, DAVID GUSELLA

100. Copyright (c) 2013 Boston College Law School Boston College Law Review, January, 2013, Boston College Law Review, 54 B.C. L. Rev 1, 35884 words, ARTICLE: FACEBOOK AND INTERPERSONAL PRIVACY: WHY THE THIRD PARTY DOCTRINE SHOULD NOT APPLY, MONU BEDI \*

101. Copyright (c) 2014 Boston College Law School Boston College Law Review, 2014, Boston College Law Review, 55 B.C. L. Rev 93, 10172 words, ARTICLE: BIG DATA AND DUE PROCESS: TOWARD A FRAMEWORK TO REDRESS PREDICTIVE PRIVACY HARMS, KATE CRAWFORD \* and JASON SCHULTZ \*\*

102. Copyright (c) 2012 Trustees of Boston University Boston University Journal of Science and Technology Law, Summer, 2012, Boston University Journal of Science & Technology Law, 18 B.U. J. SCI. & TECH. L. 262, 20488 words, ARTICLE: SUNLIGHT WITHOUT SUNBURNS: BALANCING PUBLIC ACCESS AND PRIVACY IN BALLOT MEASURE DISCLOSURE LAWS, Jacob Gardener\*

103. Copyright (c) 2011 Trustees of Boston University Boston University Journal of Science and Technology Law, Winter, 2011, Boston University Journal of Science and Technology Law, 17 B.U. J. SCI. & TECH. L. 1, 19518 words, ARTICLE: PRIVACY AND SECURITY IN THE IMPLEMENTATION OF HEALTH INFORMATION TECHNOLOGY (ELECTRONIC HEALTH RECORDS): U.S. AND EU COMPARED, Janine Hiller Professor of Business Law Pamplin College of Business Virginia Tech, Matthew S. McMullen Partner, Martinelli and McMullen Professional Services, Wade M. Chumney Cecil B. Day Assistant Professor of Business Ethics and Law Georgia Institute of Technology, David L. Baumer Department Head, Professor of Law and Technology North Carolina State University

104. Copyright (c) 2013 The Trustees of Boston University The Boston University Public Interest Law Journal, Winter, 2013, The Boston University Public Interest Law Journal, 22 B.U. Pub. Int. L.J. 1, 22898 words, ARTICLE: THE FOURTH AMENDMENT BEYOND KATZ, KYLLO AND JONES: REINSTATING JUSTIFIABLE RELIANCE AS A MORE SECURE CONSTITUTIONAL STANDARD FOR PRIVACY, Richard Sobel, Barry Horwitz, and Gerald Jenkins\*

105. Copyright (c) 2013 The Trustees of Boston University The Boston University Public Interest Law Journal, Winter, 2013, The Boston University Public Interest Law Journal, 22 B.U. Pub. Int. L.J. 45, 9664 words, ARTICLE: SOME REASONS FOR OUR AMBIVALENCE ABOUT THE VALUE OF PRIVACY, R. George Wright\*

106. Copyright (c) 2013 The Trustees of Boston University The Boston University Public Interest Law Journal, Winter, 2013, The Boston University Public Interest Law Journal, 22 B.U. Pub. Int. L.J. 67, 33307 words, ARTICLE: PROPERTY, PRIVACY AND POWER: RETHINKING THE FOURTH AMENDMENT IN THE WAKE OF U.S. V. JONES, Dr. Dana Raigrodski\*

107. Copyright (c) 2012 Brigham Young University Education and Law Journal Brigham Young University Education and Law Journal, 2012, Brigham Young University Education and Law Journal, 2012 BYU Educ. & L. J. 31, 23200 words, Article: Public Education and Student Privacy: Application of the Fourth Amendment to Dormitories at Public Colleges and Universities, Bryan R. Lemons

108. Copyright (c) 2013 Brigham Young University Law Review Brigham Young University Law Review, 2013, Brigham Young University Law Review, 2013 B.Y.U.L. Rev. 183, 14004 words, COMMENT: Walking a Thin Blue Line: Balancing the Citizen's Right to Record Police Officers Against Officer Privacy, Rebecca G. Van Tassell\*

109. Copyright (c) 2012 Brigham Young University Law Review Brigham Young University Law Review, 2012, Brigham Young University Law Review, 2012 B.Y.U.L. Rev. 343, 12331 words, COMMENT: (Un)Reasonable Expectation of Digital Privacy, Brandon T. Crowther\*

110. Copyright (c) 2012 Brigham Young University Law Review Brigham Young University Law Review, 2012, Brigham Young University Law Review, 2012 B.Y.U.L. Rev. 591, 8097 words, NOTE: Privacy Rights Left Behind at the Border: The Exhaustive, Exploratory Searches Effectuated in United States v. Cotterman, Aaron McKnight\*

111. Copyright (c) 2014 Brooklyn Journal of International Law Brooklyn Journal of International Law, 2014, Brooklyn Journal of International Law, 39 Brooklyn J. Int'l L. 269, 37414 words, ARTICLE: POSTHUMOUS REPUTATION AND POSTHUMOUS PRIVACY IN CHINA: THE DEAD, THE LAW, AND THE SOCIAL TRANSITION, Dr. Bo Zhao \*

112. Copyright (c) 2013 Brooklyn Journal of International Law Brooklyn Journal of International Law, 2013, Brooklyn Journal of International Law, 38 Brooklyn J. Int'l L. 729, 15311 words, NOTE: INDIA'S CHALLENGE: PRESERVING PRIVACY RIGHTS WHILE IMPLEMENTING AN EFFECTIVE NATIONAL IDENTIFICATION SYSTEM, Caroline E. McKenna\*

113. Copyright (c) 2011 Brooklyn Journal of International Law Brooklyn Journal of International Law, 2011, Brooklyn Journal of International Law, 37 Brooklyn J. Int'l L. 317, 15805 words, NOTE: BLURRED LINE: ZOOMING IN ON GOOGLE STREET VIEW AND THE GLOBAL RIGHT TO PRIVACY, Lauren H. Rakower \*

114. Copyright (c) 2013 Brooklyn Law Review Brooklyn Law Review, Fall, 2013, Brooklyn Law Review, 79 Brooklyn L. Rev. 175, 15763 words, ARTICLE: Comprehensive Protection of Genetic Information: ONE SIZE PRIVACY OR PROPERTY MODELS MAY NOT FIT ALL, Anya E.R. Prince +

115. Copyright (c) 2013 Brooklyn Law Review Brooklyn Law Review, Summer, 2013, Brooklyn Law Review, 78 Brooklyn L. Rev. 1279, 19317 words, ARTICLE: The Drones Are Coming! WILL THE FOURTH AMENDMENT STOP THEIR THREAT TO OUR PRIVACY?, Robert Molko +

116. Copyright (c) 2012 Brooklyn Law Review Brooklyn Law Review, Winter, 2012, Brooklyn Law Review, 77 Brooklyn L. Rev. 709, 16607 words, NOTE: Surviving an Immigration Marriage Fraud Investigation: ALL YOU NEED IS LOVE, LUCK, AND TIGHT PRIVACY CONTROLS, Samantha L. Chetrit+

117. Copyright (c) 2012 Brooklyn Law Review Brooklyn Law Review, Summer, 2012, Brooklyn Law Review, 77 Brooklyn L. Rev. 1389, 30004 words, ARTICLE: The Class Differential in Privacy Law, Michele Estrin Gilman+

118. Copyright (c) 2013 Buffalo Intellectual Property Law Journal Buffalo Intellectual Property Law Journal, Fall, 2013, Buffalo Intellectual Property Law Journal, 9 Buff. Intell. Prop. L.J. 77, 6629 words, NOTE: GEOLOCATION AND TARGETED ADVERTISING: MAKING THE CASE FOR HEIGHTENED PROTECTIONS TO ADDRESS GROWING PRIVACY CONCERNS, Ryan Mura

119. Copyright (c) 2013 Buffalo Law Review Buffalo Law Review, December, 2013, Buffalo Law Review, 61 Buffalo L. Rev. 1119, 32125 words, ARTICLE: From Privacy to Publicity: The Tort of Appropriation in the Age of Mass Consumption, Samantha Barbas+

120. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 1711, 33839 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Article: Privacy Torts: Unreliable Remedies for LGBT Plaintiffs, Anita L. Allen+

121. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 1765, 21334 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Article: Protecting Privacy in Health Research: The Limits of Individual Choice, Fred H. Cate+

122. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 1805, 26461 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Article: Mainstreaming Privacy Torts, Danielle Keats Citron+

123. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 1853, 16284 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Article: Beyond Privacy, Beyond Rights-Toward a "Systems" Theory of Information Governance, Viktor Mayer-Schonberger+

124. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 1887, 21714 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Article: Prosser's Privacy Law: A Mixed Legacy, Neil M. Richards+ and Daniel J. Solove++

125. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 1925, 36174 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Article: Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?, Paul M. Schwartz+ and Karl-Nikolaus Peifer++

126. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 1989, 8950 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Article: Privacy-An Endless Debate?, Spiros Simitis+

127. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 2007, 22864 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Article: Reunifying Privacy Law, Lior Jacob Strahilevitz+

128. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 2049, 23039 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Comment: Cracks in the Foundation of Federal Law: Ameliorating the Ongoing Mortgage Foreclosure Crisis Through Broader Predatory Lending Relief and Deterrence, Katherine M. Lehe+

129. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 2093, 16708 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Comment: Sex Offender Civil Commitment: The Treatment Paradox, Jeslyn A. Miller+

130. Copyright (c) 2010 California Law Review, Inc., a California Nonprofit Corporation California Law Review, December, 2010, California Law Review, 98 Calif. L. Rev. 2129, 15315 words, Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Essay: Our Unsettled Ninth Amendment: An Essay on Unenumerated Rights and the Impossibility of Textualism, Louis Michael Seidman+

131. Copyright (c) 2010 The Campbell Law Review Campbell Law Review, Winter, 2010, CAMPBELL LAW REVIEW, 32 Campbell L. Rev. 147, 18319 words, Article: The Danger to Confidential Communications in the Mismatch Between the Fourth Amendment's "Reasonable Expectation of Privacy" and the Confidentiality of Evidentiary Privileges, Robert P. Mosteller and Kenneth S. Broun\*

132. Copyright (c) 2013 Yeshiva University Cardozo Arts & Entertainment Law Journal, 2013, Cardozo Arts & Entertainment Law Journal, 32 Cardozo Arts & Ent LJ 83, 22417 words, ARTICLE: PROTECTING POST-MORTEM PRIVACY: RECONSIDERING THE PRIVACY INTERESTS OF THE DECEASED IN A DIGITAL WORLD<>, Lilian Edwards and Edina Harbinja\*

133. Copyright (c) 2013 Yeshiva University Cardozo Arts & Entertainment Law Journal, 2013, Cardozo Arts & Entertainment Law Journal, 32 Cardozo Arts & Ent LJ 347, 16709 words, NOTE: "A RIGHT TO BE SPARED UNHAPPINESS": n1 IMAGES OF DEATH AND THE EXPANSION OF THE RELATIONAL RIGHT OF PRIVACY<>, Catherine Leibowitz\*

134. Copyright (c) 2013 Yeshiva University Cardozo Arts & Entertainment Law Journal, 2013, Cardozo Arts & Entertainment Law Journal, 31 Cardozo Arts & Ent LJ 925, 14143 words, SPRING SYMPOSIUM: CRITICAL LEGAL STUDIES & THE POLITICIZATION OF INTELLECTUAL PROPERTY AND INFORMATION LAW: NOTE: INFORMATION OVERLOAD: WHY OMNIPRESENT TECHNOLOGY AND THE RISE OF BIG DATA SHOULDN'T SPELL THE END FOR PRIVACY AS WE KNOW IT\*, Devin W. Ness\*

135. Copyright (c) 2012 Yeshiva University Cardozo Arts & Entertainment Law Journal, 2012, Cardozo Arts & Entertainment Law Journal, 30 Cardozo Arts & Ent LJ 283, 18213 words, NOTE: INTERNET ADVERTISING AFTER SORRELL V. IMS HEALTH: A DISCUSSION ON DATA PRIVACY & THE FIRST AMENDMENT, Agatha M. Cole\*

136. Copyright (c) 2012 Yeshiva University Cardozo Journal of International and Comparative Law, Summer, 2012, Cardozo Journal of International and Comparative Law, 20 Cardozo J. Int'l & Comp. L. 571, 12201 words, SYMPOSIUM 2012: AMATEUR ATHLETICS, PROFESSIONAL IP: SYMPOSIUM: CARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW: Transcript of 20th Anniversary Symposium, March 8, 2012: Surveillance and Privacy at the London 2012 Olympics

137. Copyright (c) 2013 Yeshiva University Cardozo Law Review, December, 2013, Cardozo Law Review, 35 Cardozo L. Rev. 643, 35905 words, ARTICLE: Contextual Expectations of Privacy, Andrew D. Selbst+

138. Copyright (c) 2014 Yeshiva University Cardozo Law Review, April, 2014, Cardozo Law Review, 35 Cardozo L. Rev. 1289, 32630 words, ARTICLE: Testing the Boundaries of Family Privacy: The Special Case of Pediatric Sibling Transplants, Doriane Lambelet Coleman+

139. Copyright (c) 2011 Yeshiva University Cardozo Law Review, December, 2011, Cardozo Law Review, 33 Cardozo L. Rev. 737, 17055 words, NOTE: A Mosaic Shield: Maynard, the Fourth Amendment, and Privacy Rights in the Digital Age, Erin Smith Dennis\*

140. Copyright (c) 2012 Yeshiva University Cardozo Public Law, Policy & Ethics Journal, Spring, 2012, Cardozo Public Law, Policy & Ethics Journal, 10 Cardozo Pub. L. Pol'y & Ethics J. 357, 18970 words, NOTE: CHILDHOOD OBESITY: BALANCING THE NATION'S INTEREST WITH A PARENT'S CONSTITUTIONAL RIGHT TO PRIVACY, Denise Cohen\*

141. Copyright (c) 2013 The Cardozo School of Law of Yeshiva University Law & Literature, Spring, 2013, Law and Literature, 25 Law & Literature 85, 8151 words, SPECIAL ISSUE ON FUTURES OF FAIR USE: "Ah, you publishing scoundrel!": A Hauntological Reading of Privacy, Moral Rights, and the Fair Use of Unpublished Works, Robert Spoo

142. Copyright (c) 2011 The Cardozo School of Law of Yeshiva University Law & Literature, Spring, 2011, Law and Literature, 23 Law & Literature 1, 10930 words, ARTICLE: Inviolate Personality and the Literary Roots of the Right to Privacy, David Rosen and Aaron Santesso

143. Copyright (c) 2010 Case Western Reserve Journal of International Law Case Western Reserve Journal of International Law, 2010, Case Western Reserve Journal of International Law, 42 Case W. Res. J. Int'l L. 543, 3700 words, SOMEBODY'S WATCHING ME: SURVEILLANCE AND PRIVACY IN AN AGE OF NATIONAL INSECURITY: Foreword: Somebody's Watching Me: Surveillance and Privacy in an Age of National Insecurity, Robert N. Strassfeld\* & Cheryl Ough+

144. Copyright (c) 2010 Case Western Reserve Journal of International Law Case Western Reserve Journal of International Law, 2010, Case Western Reserve Journal of International Law, 42 Case W. Res. J. Int'l L. 551, 9664 words, SURVEILLANCE IN PUBLIC PLACES AND CLOSED CIRCUIT TELEVISION (CCTV): Article: Digital Multi-Media and the Limits of Privacy Law, Jacqueline D. Lipton\*

145. Copyright (c) 2010 Case Western Reserve Journal of International Law Case Western Reserve Journal of International Law, 2010, Case Western Reserve Journal of International Law, 42 Case W. Res. J. Int'l L. 625, 10478 words, THE GLOBALIZATION OF SURVEILLANCE: Article: Privacy and Counter-Terrorism: The Pervasiveness of Data, Paul Rosenzweig\*

146. Copyright (c) 2010 Case Western Reserve Journal of International Law Case Western Reserve Journal of International Law, 2010, Case Western Reserve Journal of International Law, 42 Case W. Res. J. Int'l L. 699, 5447 words, RESISTANCE TO SURVEILLANCE: Article: A Social Movement for Privacy/Against Surveillance? Some Difficulties in Engendering Mass Resistance in a Land of Twitter and Tweets, Laura Huey\*

147. Copyright (c) 2012 Case Western Reserve University Case Western Reserve Law Review, Spring, 2012, Case Western Reserve Law Review, 62 Case W. Res. 801, 18666 words, ARTICLE: NONPROFITS, POLITICS, AND PRIVACY, Lloyd Hitoshi Mayer +

148. Copyright (c) 2013 Charlotte School of Law, All Rights Reserved. Charlotte Law Review, Spring / Summer, 2013, Charlotte Law Review, 4 Charlotte L. Rev. 1, 20092 words, INDIVIDUAL RIGHTS: Moving Beyond a Brick and Mortar Understanding of State Action: The Case for a More Majestic State Action Doctrine to Protect Employee Privacy in the Workplace, Ronald P. Angerer II\*

149. Copyright (c) 2013 University of Chicago The University of Chicago Legal Forum, 2013, University of Chicago Legal Forum, 2013 U Chi Legal F 69, 12583 words, ARTICLE: The Constitutionality of Consumer Privacy Regulation, Felix T. Wu +

150. Copyright (c) 2013 University of Chicago The University of Chicago Legal Forum, 2013, University of Chicago Legal Forum, 2013 U Chi Legal F 173, 23374 words, ARTICLE: Regulating at the End of Privacy, Bruce E. Boyden +

151. Copyright (c) 2012 Chicago-Kent College of Law Chicago-Kent Law Review, 2012, Chicago-Kent Law Review \*, 87 Chi.-Kent L. Rev. 901, 14508 words, THE PIPER LECTURE: ELECTRONIC PRIVACY AND EMPLOYEE SPEECH, Pauline T. Kim\*

... in the organization of work and advances in technology. Current **privacy** law is illequipped to address these changes and as a result, employees' **privacy** in their electronic communications is only weakly protected from employer ...

... employer reprisals. These two developments? weak protection of employee **privacy** and increased protection for some socially valued forms of employee speech?are at odds because **privacy** and speech are closely connected. As **privacy** scholars have emphasized, protecting **privacy** promotes speech values by granting individuals space to ...

... public speech. Similarly, in the workplace context, some measure of **privacy** to explore ideas and communicate with others may be necessary to ensure that ...

... simultaneously expecting more from employee speech and protecting employee **privacy** less,even though the latter may be necessary to produce the ...

152. Copyright (c) 2011 Chicago-Kent College of Law Chicago-Kent Law Review, 2011, Chicago-Kent Law Review, 86 Chi.-Kent L. Rev. 161, 16969 words, SYMPOSIUM ON ENERGY LAW: ARTICLE: PRIVACY IMPLICATIONS OF SMART METERS, Cheryl Dancey Balough\*

153. Copyright (c) 2010 Chicago-Kent College of Law Chicago-Kent Law Review, 2010, Chicago-Kent Law Review, 84 Chi.-Kent L. Rev. 851, 3754 words, SYMPOSIUM: DATA DEVOLUTION: CORPORATE INFORMATION SECURITY, CONSUMERS, AND THE FUTURE OF REGULATION: ARTICLE: REASONS WHY WE SHOULD AMEND THE CONSTITUTION TO PROTECT PRIVACY, Deborah Pierce\*

154. Copyright (c) 2010 Chicago-Kent College of Law Chicago-Kent Law Review, 2010, Chicago-Kent Law Review, 84 Chi.-Kent L. Rev. 861, 6059 words, SYMPOSIUM: DATA DEVOLUTION: CORPORATE INFORMATION SECURITY, CONSUMERS, AND THE FUTURE OF REGULATION: ARTICLE: CODING PRIVACY, Lilian Edwards\*

155. Copyright (c) 2013 University of Cincinnati University of Cincinnati Law Review, Spring, 2013, University of Cincinnati Law Review, 81 U. Cin. L. Rev. 1027, 16150 words, Comment and Casenote: Are You on the List? Dispelling the Myth of a Total Exemption from the Privacy Act's Civil Remedies in Shearson v. DHS, Maxim Brumbach\*

156. Copyright (c) 2013 University of Cincinnati University of Cincinnati Law Review, Spring, 2013, University of Cincinnati Law Review, 81 U. Cin. L. Rev. 1127, 12001 words, Comment and Casenote: Sexual Privacy in the Modern Era: Lowe v. Swanson, Katie Rasfeld Terpstra\*

157. Copyright (c) 2011 Cleveland State University Cleveland State Law Review, 2011, Cleveland State Law Review, 59 Clev. St. L. Rev. 377, 14836 words, ARTICLE: WORKPLACE PRIVACY AND MONITORING: THE QUEST FOR BALANCED INTERESTS, ARIANA R. LEVINSON \*

158. Copyright (c) 2013 University of Colorado Law Review University of Colorado Law Review, Fall, 2013, University of Colorado Law Review, 84 U. Colo. L. Rev. 1117, 27435 words, ARTICLE: DEFINING PRIVACY AND UTILITY IN DATA SETS, Felix T. Wu\*

159. Copyright (c) 2011 University of Colorado Law Review University of Colorado Law Review, Winter, 2011, University of Colorado Law Review, 82 U. Colo. L. Rev. 307, 11460 words, COMMENT: A FUNDAMENTAL RIGHT TO READ: READER PRIVACY PROTECTIONS IN THE U.S. CONSTITUTION, Eric Robertson\*

160. Copyright (c) 2011 Columbia Human Rights Law Review Columbia Human Rights Law Review, Fall, 2011, Columbia Human Rights Law Review, 43 Colum. Human Rights L. Rev. 301, 22975 words, NOTE: RESTORING PRIVACY AT THE BORDER: EXTENDING THE REASONABLE SUSPICION STANDARD FOR LAPTOP BORDER SEARCHES, Benjamin J. Rankin \*

161. Copyright (c) 2011 Columbia Human Rights Law Review Columbia Human Rights Law Review, Spring, 2011, Columbia Human Rights Law Review, 42 Colum. Human Rights L. Rev. 759, 14259 words, ARTICLE: PRIVACY FOR CHILDREN, Benjamin Shmueli \* and Ayelet Blecher-Prigat \*\*

162. Copyright (c) 2013 European Legal Studies Center, Columbia University Columbia Journal of European Law, Spring, 2013, Columbia Journal of European Law, 19 Colum. J. Eur. L. 341, 16879 words, STUDENT NOTE: A COMPARATIVE APPROACH TO UNDERSTANDING DEVELOPMENTS IN PRIVACY RIGHTS IN THE EUROPEAN COURT OF HUMAN RIGHTS, Catherine Bratic \*

163. Copyright (c) 2014 Columbia Journal of Transnational Law Association, Inc. Columbia Journal of Transnational Law, 2014, Columbia Journal of Transnational Law, 52 Colum. J. Transnat'l L. 569, 22641 words, Note: Practicing Privacy Online: Examining Data Protection Regulations Through Google's Global Expansion, John Schinasi\*

164. Copyright (c) 2014 Directors of The Columbia Law Review Association, Inc. Columbia Law Review, April, 2014, Columbia Law Review, 114 Colum. L. Rev. 583, 16937 words, ARTICLE: THE FTC AND THE NEW COMMON LAW OF PRIVACY, Daniel J. Solove \* & Woodrow Hartzog \*\*

165. Copyright (c) 2014 Directors of The Columbia Law Review Association, Inc. Columbia Law Review, May, 2014, Columbia Law Review, 114 Colum. L. Rev. 879, 33045 words, ARTICLE: TORT LAW VS. PRIVACY, Eugene Volokh \*

166. Copyright (c) 2013 Directors of The Columbia Law Review Association, Inc. Columbia Law Review, December, 2013, Columbia Law Review, 113 Colum. L. Rev. 2227, 21719 words, NOTE: SMILE FOR THE CAMERA, THE WORLD IS GOING TO SEE THAT MUG: THE DILEMMA OF PRIVACY INTERESTS IN MUG SHOTS, Gregory Nathaniel Wolfe \*

167. Copyright (c) 2012 Columbia Science and Technology Law Review Columbia Science and Technology Law Review, Fall, 2012, Columbia Science and Technology Law Review, 14 Colum. Sci. & Tech. L. Rev. 72, 20186 words, ARTICLE: DRONES AND PRIVACY +, Timothy T. Takahashi, Ph.D. \*

168. Copyright (c) 2012 The Trustees of Columbia University in the City of New York The Columbia Journal of Law & the Arts, Fall, 2012, Columbia Journal of Law & the Arts, 36 Colum. J.L. & Arts 21, 35581 words, ARTICLE: The Sidis Case and the Origins of Modern Privacy Law, Samantha Barbas\*

169. Copyright (c) 2011 The Trustees of Columbia University in the City of New York The Columbia Journal of Law & the Arts, Summer, 2011, Columbia Journal of Law & the Arts, 34 Colum. J.L. & Arts 837, 3110 words, Symposium: Collective Management of Copyright: Solution or Sacrifice?: A Digital Public Library of America?: Collective Management's Implications for Privacy, Private Use and Fair Use, John Palfrey\*

170. Copyright (c) 2013 The Catholic University of America CommLaw Conspectus, 2013, CommLaw Conspectus, 21 CommLaw Conspectus 365, 16652 words, COMMENT: DRONES IN THE HOMELAND: A POTENTIAL PRIVACY OBSTRUCTION UNDER THE FOURTH AMENDMENT AND THE COMMON LAW TRESPASS DOCTRINE, Ajoke Oyegunle ++

171. Copyright (c) 2011 The Catholic University of America CommLaw Conspectus, 2011 - 2012, CommLaw Conspectus, 20 CommLaw Conspectus 293, 901 words, CONSPECTUS: SELECTED DOCKET AND LEGISLATIVE SUMMARIES, 2011: In re The Federal Trade Commission's Proposed Revisions to the Children's Online Privacy Protection Rule, Notice of Proposed Rulemaking, 76 Fed. Reg. 59804 (Sept. 27, 2011)., Summarized by Rebecca Borges

172. Copyright (c) 2012 The Catholic University of America CommLaw Conspectus, 2012, CommLaw Conspectus, 20 CommLaw Conspectus 415, 13218 words, COMMENT: DATA PRIVACY AND THE FOREIGN CORRUPT PRACTICES ACT: A STUDY OF ENFORCEMENT AND ITS EFFECT ON CORPORATE COMPLIANCE IN THE AGE OF GLOBAL REGULATION, Katherine Morga ++

173. Copyright (c) 2012 The Catholic University of America CommLaw Conspectus, 2012, CommLaw Conspectus, 20 CommLaw Conspectus 445, 13210 words, COMMENT: THE FUTURE OF WALLETS: A LOOK AT THE PRIVACY IMPLICATIONS OF MOBILE PAYMENTS, Meena Aharam Rajan ++

174. Copyright (c) 2010 The Catholic University of America CommLaw Conspectus, 2010, CommLaw Conspectus, 19 CommLaw Conspectus 211, 17456 words, COMMENT: The Battle Between Privacy and Policy in Quon v. City of Ontario: Employee Privacy Rights and the Operational Realities of the Workplace on Display at the Supreme Court, Carolyn G. Coda +

175. Copyright (c) 2011 The Catholic University of America CommLaw Conspectus, 2011, CommLaw Conspectus, 19 CommLaw Conspectus 297, 23027 words, ARTICLE: THE SMART GRID: THE COMPLEXITIES AND IMPORTANCE OF DATA PRIVACY AND SECURITY, H. Russell Frisby, Jr. + & Jonathan P. Trotta ++

176. Copyright (c) 2011 The Catholic University of America CommLaw Conspectus, 2011, CommLaw Conspectus, 19 CommLaw Conspectus 481, 17819 words, COMMENT: DON'T TAKE IT PERSONALLY: SUPREME COURT FINDS CORPORATIONS LACK PERSONAL PRIVACY UNDER FOIA EXEMPTIONS, Maeve E. Huggins +

177. Copyright (c) 2014 Taylor & Francis Group, LLC Communication Law and Policy, Winter, 2014, Communication Law & Policy, 19 Comm. L. & Pol'y 119, 4184 words, SUMMIT REPORT: FREEDOM OF THE PRESS IN THE TWENTY-FIRST CENTURY -- AN AGENDA FOR THOUGHT AND ACTION: PANEL III: THE FUTURE OF THE PRESS AND PRIVACY, CLAY CALVERT \*

178. Copyright (c) 2013 Taylor & Francis Group, LLC Communication Law and Policy, Winter, 2013, Communication Law & Policy, 18 Comm. L. & Pol'y 91, 16083 words, ARTICLE: FORGETTING THE FIRST AMENDMENT: HOW OBSCURITY-BASED PRIVACY AND A RIGHT TO BE FORGOTTEN ARE INCOMPATIBLE WITH FREE SPEECH, ROBERT G. LARSON III \*

179. Copyright (c) 2012 Taylor & Francis Group, LLC Communication Law and Policy, Spring, 2012, Communication Law & Policy, 17 Comm. L. & Pol'y 107, 11111 words, ESSAY: THE "NEW" PRIVACY AND THE "OLD": Is APPLYING THE TORT LAW OF PRIVACY LIKE PUTTING HIGH-BUTTON SHOES ON THE INTERNET?, DIANE LEENHEER ZIMMERMAN \*

180. Copyright (c) 2010 Taylor & Francis Group, LLC Communication Law and Policy, Autumn, 2010, Communication Law & Policy, 15 Comm. L. & Pol'y 435, 359 words, ARTICLE: CALL FOR PAPERS: The Changing Face of Privacy in the Digital Age

181. Copyright (c) 2010 Comparative Labor Law & Policy Journal Comparative Labor Law & Policy Journal, Summer, 2010, Comparative Labor Law & Policy Journal, 31 Comp. Lab. L. & Pol'y J. 705, 17300 words, ARTICLE: PROTECTION OF PRIVACY IN LABOR RELATIONS: THE ITALIAN CASE WITHIN THE EUROPEAN DIMENSION, Andrea Sitzia+ and Enrico Barraco++

182. Copyright (c) 2011 Competition Policy International, LLC All Rights Reserved. Competition Policy International, Spring, 2011, Competition Policy International, 7 Competition Pol'y Int'l 7, 7538 words, ARTICLE: The Intersection of Consumer Protection and Competition in the New World of Privacy, Julie Brill \*

183. Copyright (c) 2011 Competition Policy International, LLC All Rights Reserved. Competition Policy International, Spring, 2011, Competition Policy International, 7 Competition Pol'y Int'l 41, 8297 words, ARTICLE: Applications Want to be Free: Privacy Against Information, Michael R. Hammock & Paul H. Rubin \*

184. Copyright (c) 2011 Connecticut Public Interest Law Journal Connecticut Public Interest Law Journal, Spring / Summer, 2011, Connecticut Public Interest Law Journal, 10 Conn. Pub. Int. L.J. 355, 8651 words, SPECIAL FEATURE: PRIVACY INVASIONS & THE MEDIA: Fickle Justice: Judicial Idiosyncrasy in UK Privacy Cases, Paul Wragg+

185. Copyright (c) 2011 Connecticut Public Interest Law Journal Connecticut Public Interest Law Journal, Spring / Summer, 2011, Connecticut Public Interest Law Journal, 10 Conn. Pub. Int. L.J. 371, 6522 words, SPECIAL FEATURE: PRIVACY INVASIONS & THE MEDIA: Enjoining Selective Forced Exposure of Figures of Contemporary Society, Robin D. Barnes and Yamuna Menon+

186. Copyright (c) 2011 Connecticut Public Interest Law Journal Connecticut Public Interest Law Journal, Spring / Summer, 2011, Connecticut Public Interest Law Journal, 10 Conn. Pub. Int. L.J. 385, 7444 words, SPECIAL FEATURE: PRIVACY INVASIONS & THE MEDIA: "A Simple, Human Measure of Privacy": Public Disclosure of Private Facts in the World of Tiger Woods, Patricia Sanchez Abril+

187. Copyright (c) 2011 Connecticut Law Review CONNtemplations, Spring, 2011, CONNtemplations, 43 Conn. L. Rev. CONNtemplations 1, 4430 words, RESPONSE: Remembering Privacy and Regulation, ALFRED L. BROPHY \*

188. Copyright (c) 2011 Cornell University Cornell International Law Journal, Fall, 2011, Cornell International Law Journal, 44 Cornell Int'l L.J. 535, 18964 words, ARTICLE: A Conflict of Interests: Privacy, Truth, and Compulsory DNA Testing for Argentina's Children of the Disappeared, Elizabeth B. Ludwin King+

189. Copyright (c) 2010 Cornell University Cornell International Law Journal, Fall, 2010, Cornell International Law Journal, 43 Cornell Int'l L.J. 585, 17613 words, NOTE: Disclosing Stored Communication Data to Fight Crime: The U.S. and EU Approaches to Balancing Competing Privacy and Security Interests, Elise M. Simbro+

190. Copyright (c) 2014 Cornell University Cornell Journal of Law and Public Policy, Spring, 2014, Cornell Journal of Law and Public Policy, 23 Cornell J. L. & Pub. Pol'y 661, 14577 words, NOTE: FACEBOOK, PRIVACY, AND REASONABLE NOTICE: THE PUBLIC POLICY PROBLEMS WITH FACEBOOK'S CURRENT SIGN-UP PROCESS AND HOW TO REMEDY THE LEGAL ISSUES, Michael J. Milazzo\*

191. Copyright (c) 2012 Cornell University Cornell Journal of Law and Public Policy, Winter, 2012, Cornell Journal of Law and Public Policy, 22 Cornell J. L. & Pub. Pol'y 237, 24749 words, ARTICLE: DOCUMENTING DEATH: PUBLIC ACCESS TO GOVERNMENT DEATH RECORDS AND ATTENDANT PRIVACY CONCERNS, Jeffrey R. Boles\*

192. Copyright (c) 2014 Cornell Law Review Cornell Law Review, March, 2014, Cornell Law Review, 99 Cornell L. Rev. 633, 12537 words, NOTE: MUG SHOTS AND THE FOIA: WEIGHING THE PUBLIC'S INTEREST IN DISCLOSURE AGAINST THE INDIVIDUAL'S RIGHT TO PRIVACY, Jane E. Bobet+

193. Copyright (c) 2012 Cumberland Law Review Cumberland Law Review, 2012 / 2013, Cumberland Law Review, 43 Cumb. L. Rev. 259, 24406 words, COMMENT: THE SOCIALLY UNPOPULAR VERDICT: A POST-CASEY ANTHONY ANALYSIS OF THE NEED TO REFORM JUROR PRIVACY POLICY, Clinton T. Speegle n1

194. Copyright (c) 2012 Cumberland Law Review Cumberland Law Review, 2012 - 2013, Cumberland Law Review, 43 Cumb. L. Rev. 495, 18677 words, COMMENT: BARENAKED LADIES AND THE BONA FIDE OCCUPATIONAL QUALIFICATION: THE INTERSECTION OF GENDER AND PRIVACY IN PERMISSIBLE SEX DISCRIMINATION, RACHEL STEWART MARTIN n1

195. Copyright (c) 2010 University of Dayton Law Review University of Dayton Law Review, Spring, 2010, University of Dayton Law Review, 35 Dayton L. Rev. 345, 11699 words, ARTICLE: MODEL OMNIBUS PRIVACY STATUTE, Scot Ganow, J.D., CIPP n1 Sam S. Han, Ph.D. n2

196. Copyright (c) 2010 Denver University Law Review Denver University Law Review, 2010, Denver University Law Review, 87 Denv. U.L. Rev. 747, 14564 words, SURVEY: Propping up the Illusion of Computer Privacy in United States v. Burgess, Darren Kafka\*

197. Copyright (c) 2012 DePaul University DePaul Law Review, Spring, 2012, DePaul Law Review, 61 DePaul L. Rev. 869, 19589 words, SYMPOSIUM: CHANGING CONCEPTIONS: EXPLORING THE MEDICAL AND LEGAL ADVANCES IN FERTILITY PRESERVATION: TWENTY-FIRST ANNUAL LAW REVIEW SYMPOSIUM: COMMENT: NEWBORN SCREENING PROGRAMS: HOW DO WE BEST PROTECT PRIVACY RIGHTS WHILE ENSURING OPTIMAL NEWBORN HEALTH?, Rachel L. Schweers, Ph.D.\*

198. Copyright (c) 2012 DePaul University DePaul Law Review, Summer, 2012, DePaul Law Review, 61 DePaul L. Rev. 973, 41324 words, ARTICLE: SAVING PRIVACY FROM HISTORY, Samantha Barbas\*

199. Copyright (c) 2011 DePaul University DePaul Law Review, Spring, 2011, DePaul Law Review, 60 DePaul L. Rev. 895, 24941 words, SYMPOSIUM: TRIAL 2010: A LOOK INSIDE OUR NATION'S COURTROOMS: TWENTIETH ANNUAL DEPAUL LAW REVIEW SYMPOSIUM: COMMENT: BALANCING EXPECTATIONS OF ONLINE PRIVACY: WHY INTERNET PROTOCOL (IP) ADDRESSES SHOULD BE PROTECTED AS PERSONALLY IDENTIFIABLE INFORMATION, Joshua J. McIntyre\*

200. Copyright (c) 2014 DePaul University DePaul Journal of Art, Technology & Intellectual Property Law, Spring, 2014, DePaul Journal of Art, Technology & Intellectual Property Law, 24 DePaul J. Art Tech. & Intell. Prop. L. 339, 12195 words, LEGISLATIVE UPDATE: BAND-AID ON A BULLET WOUND: WHY THE EMAIL PRIVACY ACT IS NECESSARY TRIAGE IN FEDERAL TECHNOLOGY LAW, Bridget Dempsey\*

201. Copyright (c) 2013 University of Detroit Mercy School of Law University of Detroit Mercy Law Review, Winter, 2013, University of Detroit Mercy Law Review, 90 U. Det. Mercy L. Rev. 179, 13219 words, ARTICLE: Expansion of the Katz Reasonable Expectation of Privacy Test Is Necessary to Perpetuate a Majoritarian View of the Reasonable Expectation of Privacy in Electronic Communications to Third Parties, Samantha Arrington\*

202. Copyright (c) 2011 University of Detroit Mercy School of Law University of Detroit Mercy Law Review, Spring, 2011, University of Detroit Mercy Law Review, 88 U. Det. Mercy L. Rev. 555, 16366 words, NOTE: Student Athletes and the Deprivation of Rights of Privacy and Publicity - Are Fantasy Sports Leagues Infringing Upon the Rights of College Athletes? If so, What Constitutes a Viable Solution?, Leah M. Chamberlin

203. Copyright (c) 2012 National Italian American Bar Association The Digest National Italian American Bar Association Law Journal, 2012, The Digest National Italian American Bar Association Law Journal, 20 Digest 41, 5503 words, ARTICLE: Italy--Journalists, Privacy and a Right to Information, Elizabeth F. Defeis\*

204. Copyright (c) 2012 Drake University Drake Law Review, Fall, 2012, Drake Law Review, 61 Drake L. Rev. 225, 12248 words, NOTE: RECONCILING PRIVACY WITH PROGRESS: FOURTH AMENDMENT PROTECTION OF E-MAIL STORED WITH AND SENT THROUGH A THIRD-PARTY INTERNET SERVICE PROVIDER, Spencer S. Cady\*

205. Copyright © 2012 Drexel University. All Rights Reserved. Drexel Law Review, Spring, 2012, Drexel Law Review, 4 Drexel L. Rev. 487, 31242 words, NOTE: PRIVACY IN THE CLOUD FRONTIER: ABANDONING THE "TAKE IT OR LEAVE IT" APPROACH, Scott Bender \*

206. Copyright (c) 2010 Duke University Law School. All Rights Reserved. Duke Journal of Constitutional Law & Public Policy Sidebar, 2010, Duke Journal of Constitutional Law & Public Policy Sidebar, 6 Duke J. Const. Law & PP Sidebar 1, 10956 words, ARTICLE: THE CONSTITUTIONAL RIGHT TO INFORMATIONAL PRIVACY: NASA V. NELSON, RUSSELL T. GORKIN \*

207. Copyright (c) 2010 Duke Law & Technology Review Duke Law & Technology Review, 2010, Duke Law & Technology Review, 2010 Duke L. & Tech. Rev. 8, 14387 words, ARTICLE: THE ANONYMOUS POSTER: HOW TO PROTECT INTERNET USERS' PRIVACY AND PREVENT ABUSE, SCOTT NESS n1

208. Copyright (c) 2010 Duke Law & Technology Review Duke Law & Technology Review, September 28, 2010, Duke Law & Technology Review, 2010 Duke L. & Tech. Rev. 14, 16794 words, ARTICLE: PRIVACY EXPECTATIONS AND PROTECTIONS FOR TEACHERS IN THE INTERNET AGE, EMILY H. FULMER n1

209. Copyright © 2012 Elon University School of Law. All Rights Reserved. Elon Law Review, February, 2012, Elon Law Review, 3 Elon L. Rev. 133, 24995 words, ARTICLE: THE PRIVACY IMPLICATIONS OF DIGITAL PRESERVATION: SOCIAL MEDIA ARCHIVES AND THE SOCIAL NETWORKS THEORY OF PRIVACY, JASMINE MCNEALY \*

210. Copyright © 2012 Elon University School of Law. All Rights Reserved. Elon Law Review, February, 2012, Elon Law Review, 3 Elon L. Rev. 161, 14927 words, ARTICLE: PRIVACY, COPYRIGHT, AND LETTERS, JEFFREY L. HARRISON \*

211. Copyright (c) 2011 Emory Law Journal Emory Law Journal, 2011, Emory Law Journal, 61 Emory L.J. 265, 40757 words, ARTICLE: IN DEFENSE OF INDIVIDUAL TAX PRIVACY, Joshua D. Blank\*

212. Copyright (c) 2012 Chicago-Kent College of Law and Workplace Fairness Employee Rights and Employment Policy Journal, 2012, Employee Rights & Employment Policy Journal, 16 Empl. Rts. & Employ. Pol'y J. 465, 14377 words, PAPERS FROM THE AMERICAN BAR FOUNDATION - THE LABOR LAW GROUP CONFERENCE ON THE PROPOSED RESTATEMENT OF EMPLOYMENT LAW: AN EXCURSION THROUGH STRANGE TERRAIN: CHAPTERS 6 (DEFAMATION) AND 7 (PRIVACY AND AUTONOMY), By Matthew W. Finkin\*

213. Copyright (c) 2010 Chicago-Kent College of Law and Workplace Fairness Employee Rights and Employment Policy Journal, 2010, Employee Rights & Employment Policy Journal, 14 Empl. Rts. & Employ. Pol'y J. 11, 18620 words, SPECIAL ISSUE IN HONOR OF CLYDE W. SUMMERS: ARTICLE: SOME FURTHER THOUGHTS ON THE USEFULNESS OF COMPARATIVISM IN THE LAW OF EMPLOYEE PRIVACY, By Matthew W. Finkin\*

214. Copyright (c) 2010 The Federal Circuit Bar Association The Federal Circuit Bar Journal, 2010, The Federal Circuit Bar Journal, 20 Fed. Cir. B.J. 169, 13331 words, ARTICLE: Differing Perspectives: Doe v. Department of Justice: Adverse Actions for Off-Duty Conduct: Why the Federal Circuit's Approach Infringes Employees' Privacy Rights, Daniel Singer \*

215. Copyright (c) 2012 North Carolina Law Review Association First Amendment Law Review, Fall, 2012, First Amendment Law Review, 11 First Amend. L. Rev. 16, 25488 words, ARTICLE: PRIVACY AND THE RIGHT OF FREE EXPRESSION, John A. Humbach\*

216. Copyright (c) 2013 North Carolina Law Review Association First Amendment Law Review, Spring, 2013, First Amendment Law Review, 11 First Amend. L. Rev. 490, 19629 words, NOTE: Striking a Balance: Freedom of the Press Versus Children's Privacy Interests in Juvenile Dependency Hearings, Kelly Crecco\*

217. Copyright (c) 2011 North Carolina Law Review Association First Amendment Law Review, Spring, 2011, First Amendment Law Review, 9 First Amend. L. Rev. 487, 23005 words, Article: POLICE PRIVACY IN THE IPHONE ERA?: THE NEED FOR SAFEGUARDS IN STATE WIRETAPPING STATUTES TO PRESERVE THE CIVILIAN'S RIGHT TO RECORD PUBLIC POLICE ACTIVITY, By Jesse Harlan Alderman\*

218. Copyright (c) 2011 Florida Coastal Law Review Florida Coastal Law Review, Fall, 2011, Florida Coastal Law Review, 13 Fl. Coastal L. Rev. 33, 21176 words, ARTICLE: PRIVACY DISTORTION RATIONALE FOR REINTERPRETING THE THIRD-PARTY DOCTRINE OF THE FOURTH AMENDMENT, Saby Ghoshray \*

219. Copyright (c) 2011 Fordham Intellectual Property, Media & Entertainment Law Journal Fordham Intellectual Property, Media & Entertainment Law Journal, Fall, 2011, Fordham Intellectual Property, Media & Entertainment Law Journal, 22 Fordham Intell. Prop. Media & Ent. L.J. 69, 9915 words, ARTICLE: Breaking Through the "Tower of Babel": A "Right to be Forgotten" n1 and How Trans-Systemic n2 Thinking Can Help Re-Conceptualize Privacy Harm in the Age of Analytics, Karen Eltis\*

220. Copyright (c) 2011 Fordham Intellectual Property, Media & Entertainment Law Journal Fordham Intellectual Property, Media & Entertainment Law Journal, Fall, 2011, Fordham Intellectual Property, Media & Entertainment Law Journal, 22 Fordham Intell. Prop. Media & Ent. L.J. 191, 24033 words, NOTE: Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy, Christian Levis\*

221. Copyright (c) 2010 Fordham Intellectual Property, Media & Entertainment Law Journal Fordham Intellectual Property, Media & Entertainment Law Journal, Spring, 2010, Fordham Intellectual Property, Media & Entertainment Law Journal, 20 Fordham Intell. Prop. Media & Ent. L.J. 1049, 26921 words, NOTE: Friending Privacy: Toward Self-Regulation of Second Generation Social Networks, Robert Terenzi, Jr.\*

222. Copyright (c) 2012 Fordham Law Review Fordham Law Review, December, 2012, Fordham Law Review, 81 Fordham L. Rev. 1187, 14250 words, COLLOQUIUM: THE NATURAL LAW ORIGINS OF THE AMERICAN RIGHT TO PRIVACY: NATURAL LAW, SLAVERY, AND THE RIGHT TO PRIVACY TORT, Anita L. Allen\*

223. Copyright (c) 2012 Fordham Law Review Fordham Law Review, December, 2012, Fordham Law Review, 81 Fordham L. Rev. 1217, 2155 words, COLLOQUIUM: THE NATURAL LAW ORIGINS OF THE AMERICAN RIGHT TO PRIVACY: VALUING PRIVACY, Youngjae Lee\*

224. Copyright (c) 2012 Fordham Law Review Fordham Law Review, March, 2012, Fordham Law Review, 80 Fordham L. Rev. 1525, 7603 words, THE ROBERT L. LEVINE DISTINGUISHED LECTURE: THE DECIDERS: THE FUTURE OF PRIVACY AND FREE SPEECH IN THE AGE OF FACEBOOK AND GOOGLE, Jeffrey Rosen\*

225. Copyright (c) 2010 Fordham Law Review Fordham Law Review, October, 2010, Fordham Law Review, 79 Fordham L. Rev. 1, 12083 words, JUDICIAL CONFERENCE PRIVACY SUBCOMMITTEE: CONFERENCE ON PRIVACY AND INTERNET ACCESS TO COURT FILES\* PANEL ONE: GENERAL DISCUSSION ON PRIVACY AND PUBLIC ACCESS TO COURT FILES: OPENING REMARKS, Hon. Reena Raggi\*\*; Moderator Daniel J. Capra\*\*\*; Panelists Joel Reidenberg n1 Ronald Hedges n2 Peter Winn n3 Lucy Dalglish n4 Hon. Cecelia G. Morris n5 Maeva Marcus n6

226. Copyright (c) 2010 Fordham Law Review Fordham Law Review, October, 2010, Fordham Law Review, 79 Fordham L. Rev. 25, 10545 words, JUDICIAL CONFERENCE PRIVACY SUBCOMMITTEE: CONFERENCE ON PRIVACY AND INTERNET ACCESS TO COURT FILES: PANEL TWO: SHOULD THERE BE REMOTE PUBLIC ACCESS TO COURT FILINGS IN IMMIGRATION CASES?, Moderator Hon. Robert Hinkle\*; Panelists David McCraw n1 Daniel Kanstroom n2 Eleanor Acer n3 Elizabeth Cronin n4 Mark Walters n5

227. Copyright (c) 2010 Fordham Law Review Fordham Law Review, October, 2010, Fordham Law Review, 79 Fordham L. Rev. 45, 9154 words, JUDICIAL CONFERENCE PRIVACY SUBCOMMITTEE: CONFERENCE ON PRIVACY AND INTERNET ACCESS TO COURT FILES: PANEL THREE: IMPLEMENTATION--WHAT METHODS, IF ANY, CAN BE EMPLOYED TO PROMOTE THE EXISTING RULES' ATTEMPTS TO PROTECT PRIVATE IDENTIFIER INFORMATION FROM INTERNET ACCESS?, Moderator Hon. Ronald Leighton\*; Speaker Joe Cecil\*\*; Panelists Michel Ishakian n1 Edward Felten n2 Hon. Elizabeth Stong n3 Jay Safer n4 Robert Heinemann n5 Joseph Goldstein n6

228. Copyright (c) 2010 Fordham Law Review Fordham Law Review, October, 2010, Fordham Law Review, 79 Fordham L. Rev. 65, 9282 words, JUDICIAL CONFERENCE PRIVACY SUBCOMMITTEE: CONFERENCE ON PRIVACY AND INTERNET ACCESS TO COURT FILES: PANEL FOUR: COOPERATION AND PLEA AGREEMENTS--PROFESSORS & PRACTITIONERS, MODERATOR Hon. Steven Merryday\*; Panelists Caren Myers Morrison n1 Gerald Shargel n2 Barbara Sale n3 Christopher Brown n4 Alan Vinegrad n5 Jan Rostal n6 Cris Arguedas n7

229. Copyright (c) 2010 Fordham Law Review Fordham Law Review, October, 2010, Fordham Law Review, 79 Fordham L. Rev. 85, 7113 words, JUDICIAL CONFERENCE PRIVACY SUBCOMMITTEE: CONFERENCE ON PRIVACY AND INTERNET ACCESS TO COURT FILES: PANEL FIVE: COOPERATION AND PLEA AGREEMENTS--JUDGES ROUNDTABLE, MODERATOR Hon. Steven Merryday\*; Panelists Hon. Raymond Dearie n1 Hon. Loretta Preska n2 Hon. K. Michael Moore n3 Hon. Henry T. Wingate n4 Hon. Michael Baylson n5 Hon. Stefan Underhill n6

230. Copyright (c) 2010 Fordham Law Review Fordham Law Review, October, 2010, Fordham Law Review, 79 Fordham L. Rev. 99, 7849 words, JUDICIAL CONFERENCE PRIVACY SUBCOMMITTEE: CONFERENCE ON PRIVACY AND INTERNET ACCESS TO COURT FILES: PANEL SIX: TRANSCRIPTS (INCLUDING VOIR DIRE TRANSCRIPTS), MODERATOR Hon. John Koeltl\*; Panelists Hon. Gary Lancaster n1 Hon. Randolph Treece n2 Victor Kovner n3 Nora Dannehy n4 Ben Campbell n5 Lori McCarthy n6

231. Copyright (c) 2014 Fordham Urban Law Journal Fordham Urban Law Journal, May, 2014, Fordham Urban Law Journal, 41 Fordham Urb. L.J. 1349, 25433 words, UNTIL CIVIL GIDEON: EXPANDING ACCESS TO JUSTICE: NOTE: SECURING THE SMART GRID: PROTECTING NATIONAL SECURITY AND PRIVACY THROUGH MANDATORY, ENFORCEABLE INTEROPERABILITY STANDARDS, Christopher Bosch \*

232. Copyright (c) 2010 Fordham Urban Law Journal Fordham Urban Law Journal, December, 2010, Fordham Urban Law Journal, 38 Fordham Urb. L.J. 571, 32215 words, Note: BACK TO KATZ: REASONABLE EXPECTATION OF PRIVACY IN THE FACEBOOK AGE, Haley Plourde-Cole\*

233. Copyright (c) 2013 George Mason Law Review George Mason Law Review, Fall, 2013, George Mason Law Review, 21 Geo. Mason L. Rev. 117, 23167 words, ARTICLE: THE PSYCHOTHERAPIST PRIVILEGE: PRIVACY AND "GARDEN VARIETY" EMOTIONAL DISTRESS, Helen A. Anderson\*

234. Copyright (c) 2013 George Mason Law Review George Mason Law Review, Summer, 2013, George Mason Law Review, 20 Geo. Mason L. Rev. 1003, 2818 words, 16TH ANNUAL ANTITRUST SYMPOSIUM JANUARY 17, 2013: Featuring Remarks and Articles by Speakers and Panelists from the Symposium on Antitrust Law, "Privacy Regulation and Antitrust," held January 17, 2013, in the Founders Hall Auditorium at George Mason University School of Law: REMARK: KEEPING GOOGLE GOOD: REMARKS ON PRIVACY REGULATION AND FREE SPEECH, Jeffrey Rosen\*

235. Copyright (c) 2013 George Mason Law Review George Mason Law Review, Summer, 2013, George Mason Law Review, 20 Geo. Mason L. Rev. 1009, 6807 words, 16TH ANNUAL ANTITRUST SYMPOSIUM JANUARY 17, 2013: Featuring Remarks and Articles by Speakers and Panelists from the Symposium on Antitrust Law, "Privacy Regulation and Antitrust," held January 17, 2013, in the Founders Hall Auditorium at George Mason University School of Law: ARTICLE: PRIVACY, ANTITRUST, AND POWER, Frank Pasquale\*

236. Copyright (c) 2013 George Mason Law Review George Mason Law Review, Summer, 2013, George Mason Law Review, 20 Geo. Mason L. Rev. 1025, 10049 words, 16TH ANNUAL ANTITRUST SYMPOSIUM JANUARY 17, 2013: Featuring Remarks and Articles by Speakers and Panelists from the Symposium on Antitrust Law, "Privacy Regulation and Antitrust," held January 17, 2013, in the Founders Hall Auditorium at George Mason University School of Law: ARTICLE: THE IMPLICATIONS OF IMPROVED ATTRIBUTION AND MEASURABILITY FOR ANTITRUST AND PRIVACY IN ONLINE ADVERTISING MARKETS, Catherine Tucker\*

237. Copyright (c) 2013 George Mason Law Review George Mason Law Review, Summer, 2013, George Mason Law Review, 20 Geo. Mason L. Rev. 1055, 26453 words, 16TH ANNUAL ANTITRUST SYMPOSIUM JANUARY 17, 2013: Featuring Remarks and Articles by Speakers and Panelists from the Symposium on Antitrust Law, "Privacy Regulation and Antitrust," held January 17, 2013, in the Founders Hall Auditorium at George Mason University School of Law: ARTICLE: A FRAMEWORK FOR BENEFIT-COST ANALYSIS IN DIGITAL PRIVACY DEBATES, Adam Thierer\*

238. Copyright (c) 2013 George Mason Law Review George Mason Law Review, Summer, 2013, George Mason Law Review, 20 Geo. Mason L. Rev. 1107, 11266 words, 16TH ANNUAL ANTITRUST SYMPOSIUM JANUARY 17, 2013: Featuring Remarks and Articles by Speakers and Panelists from the Symposium on Antitrust Law, "Privacy Regulation and Antitrust," held January 17, 2013, in the Founders Hall Auditorium at George Mason University School of Law: ARTICLE: ANOTHER LOOK AT PRIVACY, Allen P. Grunes\*

239. Copyright (c) 2013 George Mason Law Review George Mason Law Review, Summer, 2013, George Mason Law Review, 20 Geo. Mason L. Rev. 1129, 8747 words, 16TH ANNUAL ANTITRUST SYMPOSIUM JANUARY 17, 2013: Featuring Remarks and Articles by Speakers and Panelists from the Symposium on Antitrust Law, "Privacy Regulation and Antitrust," held January 17, 2013, in the Founders Hall Auditorium at George Mason University School of Law: ARTICLE: PRIVACY AND ANTITRUST: UNDERPANTS GNOMES, THE FIRST AMENDMENT, AND SUBJECTIVITY, James C. Cooper\*

240. Copyright (c) 2012 George Mason Law Review George Mason Law Review, Spring, 2012, George Mason Law Review, 19 Geo. Mason L. Rev. 775, 19778 words, COMMENT: KEEP RECORDING: WHY ON-DUTY POLICE OFFICERS DO NOT HAVE A PROTECTED EXPECTATION OF PRIVACY UNDER MARYLAND'S STATE WIRETAP ACT, Carly Humphrey\*

241. Copyright (c) 2012 The George Washington University George Washington International Law Review, 2012, George Washington International Law Review \*, 44 Geo. Wash. Int'l L. Rev. 643, 27860 words, ARTICLE: PRIVACY IN THE AGE OF THE HACKER: BALANCING GLOBAL PRIVACY AND DATA SECURITY LAW, McKay Cunningham\*

242. Copyright (c) 2010 The George Washington University George Washington International Law Review, 2010, George Washington International Law Review, 42 Geo. Wash. Int'l L. Rev. 659, 14045 words, NOTE: A NEW AGE OF PRIVACY PROTECTION: A PROPOSAL FOR AN INTERNATIONAL PERSONAL DATA PRIVACY TREATY, Ariel E. Wade\*

243. Copyright (c) 2013 The George Washington Law Review The George Washington Law Review, December, 2013, The George Washington Law Review, 82 Geo. Wash. L. Rev. 207, 20524 words, Note: Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat Through Interagency Coordination, Patrice Hendriksen\*

244. Copyright (c) 2013 The George Washington Law Review The George Washington Law Review, August, 2013, The George Washington Law Review, 81 Geo. Wash. L. Rev. 1529, 64430 words, Annual Review of Administrative Law: Article: Privacy in Europe: Initial Data on Governance Choices and Corporate Practices, Kenneth A. Bamberger\* and Deirdre K. Mulligan\*\*

245. Copyright (c) 2011 The George Washington Law Review The George Washington Law Review, November, 2011, The George Washington Law Review, 80 Geo. Wash. L. Rev. 274, 19855 words, NOTE: Policing the Police: Freedom of the Press, the Right to Privacy, and Civilian Recordings of Police Activity, Marianne F. Kies\*

246. Copyright (c) 2012 The George Washington Law Review The George Washington Law Review, June, 2012, The George Washington Law Review, 80 Geo. Wash. L. Rev. 1209, 23197 words, Note: Privacy Is the Problem: United States v. Maynard and a Case for a New Regulatory Model for Police Surveillance, Matthew Radler\*

247. Copyright (c) 2010 The George Washington Law Review The George Washington Law Review, June, 2010, The George Washington Law Review, 78 Geo. Wash. L. Rev. 822, 10992 words, Essay: Fulfilling Government 2.0's Promise with Robust Privacy Protections, Danielle Keats Citron\*

248. Copyright (c) 2013 Georgetown Journal of International Law Georgetown Journal of International Law, Winter, 2013, Georgetown Journal of International Law, 44 Geo. J. Int'l L. 365, 24198 words, ARTICLE: THE NEW AMERICAN PRIVACY, RICHARD J. PELTZ-STEELE \*

249. Copyright (c) 2012 Georgetown Journal of Legal Ethics Georgetown Journal of Legal Ethics, Summer, 2012, Georgetown Journal of Legal Ethics, 25 Geo. J. Legal Ethics 623, 12844 words, Trust, Respect, and Cooperation May Keep Us Out of Jail: A Practical Guide to Navigating the European Union Privacy Directive's Restrictions on American Discovery Procedure, BENJAMIN L. KLEIN \*

250. Copyright (c) 2013 Georgetown Journal on Poverty Law & Policy Georgetown Journal on Poverty Law & Policy, Fall, 2013, Georgetown Journal on Poverty Law & Policy, 21 Geo. J. Poverty Law & Pol'y 1, 10489 words, ARTICLE: Taxing Privacy, Hayes Holderness \*

251. Copyright (c) 2013 Georgetown Law Journal Georgetown Law Journal, January, 2013, Georgetown Law Journal, 101 Geo. L.J. 493, 14780 words, ARTICLE: Hiding Behind Ivory Towers: Penalizing Schools That Improperly Invoke Student Privacy To Suppress Open Records Requests, ROB SILVERBLATT \*

252. Copyright (c) 2012 Georgetown Law Journal Georgetown Law Journal, August, 2012, Georgetown Law Journal, 100 Geo. L.J. 2225, 13446 words, NOTE: Failed Justifications: Why Privacy and Federalism Do Not Support the Ban on a Federal Unit-Record System, NATHANIEL B. CUSTER \*

253. Copyright (c) 2010 Georgetown Law Journal Georgetown Law Journal, April, 2010, Georgetown Law Journal, 98 Geo. L.J. 1195, 23681 words, NOTE: Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, WILLIAM JEREMY ROBISON \*

254. Copyright (c) 2013 Georgia Law Review Association, Inc. Georgia Law Review, Winter, 2013, Georgia Law Review, 47 Ga. L. Rev. 445, 32358 words, ARTICLE: GENETIC PRIVACY & THE FOURTH AMENDMENT: UNREGULATED SURREPTITIOUS DNA HARVESTING, Albert E. Scherr\*

255. Copyright (c) 2012 Georgia Law Review Association, Inc. Georgia Law Review, Spring, 2012, Georgia Law Review, 46 Ga. L. Rev. 657, 16868 words, INFORMATION PRIVACY: CHAIN-LINK CONFIDENTIALITY, Woodrow Hartzog\*

256. Copyright (c) 2012 Georgia Law Review Association, Inc. Georgia Law Review, Spring, 2012, Georgia Law Review, 46 Ga. L. Rev. 705, 5444 words, INFORMATION PRIVACY: GINA, PRIVACY, AND ANTISUBORDINATION, Bradley A. Areheart\*

257. Copyright (c) 2010 Georgia Law Review Association, Inc. Georgia Law Review, Winter, 2010, GEORGIA LAW REVIEW, 44 Ga. L. Rev. 545, 14474 words, NOTE: THE PRIVACY IMPLICATIONS OF DEEP PACKET INSPECTION TECHNOLOGY: WHY THE NEXT WAVE IN ONLINE ADVERTISING SHOULDN'T ROCK THE SELF-REGULATORY BOAT, Robert Todd Graham Collins

258. Copyright (c) 2012 Georgia State University Georgia State University Law Review, Winter, 2012, Georgia State University Law Review, 28 Ga. St. U.L. Rev. 499, 12767 words, NOTE & COMMENT: CLOUD COMPUTING: THE NEXT GREAT TECHNOLOGICAL INNOVATION, THE DEATH OF ONLINE PRIVACY, OR BOTH?, Derek Constantine \*

259. Copyright (c) 2014 Golden Gate University Golden Gate University Law Review, April, 2014, Golden Gate University Law Review, 44 Golden Gate U.L. Rev. 81, 10581 words, NOTE: NARROWLY RESTRICTING "CLEARLY ESTABLISHED" CIVIL LIBERTIES: THE CONSTITUTIONAL RAMIFICATIONS OF A FAMILY MEMBER'S UNDERPROTECTED FEDERAL PRIVACY RIGHTS IN THE DISSEMINATION OF POSTMORTEM IMAGES IN MARSH V. COUNTY OF SAN DIEGO., MAHIRA SIDDIQUI\*

260. Copyright (c) 2013 Golden Gate University Golden Gate University Law Review, Summer, 2013, Golden Gate University Law Review, 43 Golden Gate U.L. Rev. 459, 13141 words, COMMENT: LOCATION, LOCATION, LOCATION: UPDATING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT TO PROTECT GEOLOCATIONAL DATA, Alexandra D. Vesalga\*

261. Copyright (c) 2011 Golden Gate University Golden Gate University Law Review, Spring, 2011, Golden Gate University Law Review, 41 Golden Gate U.L. Rev. 299, 13553 words, NOTE: UNITED STATES v. PINEDA-MORENO: TRACKING DOWN INDIVIDUALS' REASONABLE EXPECTATION OF PRIVACY IN THE INFORMATION AGE, Caitlin Emmett\*

262. Copyright (c) 2010 Hamline Law Review Hamline Law Review, 2010, Hamline Law Review, 33 Hamline L. Rev. 95, 22879 words, COMMENT: To Impound or Not to Impound: Why Courts Need To Define Legitimate Impoundment Purposes To Restore Fourth Amendment Privacy Rights to Motorists, Chad Carr\*

263. Copyright (c) 2011 President and Fellows of Harvard College Harvard Journal of Law & Gender, Winter, 2011, Harvard Journal of Law and Gender, 34 Harv. J.L. & Gender 113, 25051 words, ARTICLE: PRIVACY RIGHTS AND PUBLIC FAMILIES, Khiara M. Bridges\*

264. Copyright (c) 2013 Harvard Society for Law & Public Policy, Inc. Harvard Journal of Law & Public Policy, Spring, 2013, Harvard Journal of Law & Public Policy, 36 Harv. J.L. & Pub. Pol'y 403, 2432 words, PRIVACY, SECURITY, AND HUMAN DIGNITY IN THE DIGITAL AGE: FOREWORD: ACCOUNTING FOR TECHNOLOGICAL CHANGE, ORIN S. KERR \*

265. Copyright (c) 2013 Harvard Society for Law & Public Policy, Inc. Harvard Journal of Law & Public Policy, Spring, 2013, Harvard Journal of Law & Public Policy, 36 Harv. J.L. & Pub. Pol'y 409, 19780 words, PRIVACY, SECURITY, AND HUMAN DIGNITY IN THE DIGITAL AGE: THE PURSUIT OF PRIVACY IN A WORLD WHERE INFORMATION CONTROL IS FAILING, ADAM THIERER \*

266. Copyright (c) 2013 Harvard Society for Law & Public Policy, Inc. Harvard Journal of Law & Public Policy, Spring, 2013, Harvard Journal of Law & Public Policy, 36 Harv. J.L. & Pub. Pol'y 457, 28189 words, PRIVACY, SECURITY, AND HUMAN DIGNITY IN THE DIGITAL AGE: OBSERVATIONS FROM ABOVE: UNMANNED AIRCRAFT SYSTEMS AND PRIVACY, JOHN VILLASENOR \*

267. Copyright (c) 2013 Harvard Society for Law & Public Policy, Inc. Harvard Journal of Law & Public Policy, Spring, 2013, Harvard Journal of Law & Public Policy, 36 Harv. J.L. & Pub. Pol'y 519, 14215 words, PRIVACY, SECURITY, AND HUMAN DIGNITY IN THE DIGITAL AGE: COMPULSORY PROCESS IN CYBERSPACE: RETHINKING PRIVACY IN THE SOCIAL NETWORKING AGE, ROBERT D. RICHARDS \*

268. Copyright (c) 2013 Harvard Society for Law & Public Policy, Inc. Harvard Journal of Law & Public Policy, Spring, 2013, Harvard Journal of Law & Public Policy, 36 Harv. J.L. & Pub. Pol'y 549, 23430 words, PRIVACY, SECURITY, AND HUMAN DIGNITY IN THE DIGITAL AGE: ENDING THE ZERO-SUM GAME: HOW TO INCREASE THE PRODUCTIVITY OF THE FOURTH AMENDMENT, RIC SIMMONS \*

269. Copyright (c) 2013 Harvard Society for Law & Public Policy, Inc. Harvard Journal of Law & Public Policy, Spring, 2013, Harvard Journal of Law & Public Policy, 36 Harv. J.L. & Pub. Pol'y 605, 25315 words, PRIVACY, SECURITY, AND HUMAN DIGNITY IN THE DIGITAL AGE: UPDATING THE LAW OF INFORMATION PRIVACY: THE NEW FRAMEWORK OF THE EUROPEAN UNION, MARC ROTENBERG \* & DAVID JACOBS \*\*

270. Copyright (c) 2013 Harvard Society for Law & Public Policy, Inc. Harvard Journal of Law & Public Policy, Spring, 2013, Harvard Journal of Law & Public Policy, 36 Harv. J.L. & Pub. Pol'y 653, 25927 words, PRIVACY, SECURITY, AND HUMAN DIGNITY IN THE DIGITAL AGE: NEUROSCIENCE, MENTAL PRIVACY, AND THE LAW, FRANCIS X. SHEN \*

271. Copyright (c) 2011 Harvard Society for Law & Public Policy, Inc. Harvard Journal of Law & Public Policy, Spring, 2011, Harvard Journal of Law & Public Policy, 34 Harv. J.L. & Pub. Pol'y 705, 29658 words, ARTICLE: DAMAGES UNDER THE PRIVACY ACT: SOVEREIGN IMMUNITY AND A CALL FOR LEGISLATIVE REFORM, ALEX KARDON \*

272. Copyright (c) 2012 by the President and Fellows of Harvard College Harvard Journal of Law & Technology, Fall, 2012, Harvard Journal of Law & Technology, 26 Harv. J. Law & Tec 165, 10426 words, ARTICLE: A FACE TELLS MORE THAN A THOUSAND POSTS: DEVELOPING FACE RECOGNITION PRIVACY IN SOCIAL NETWORKS, Yana Welinder \*

273. Copyright (c) 2011 by the President and Fellows of Harvard College Harvard Journal of Law & Technology, Fall, 2011, Harvard Journal of Law & Technology, 25 Harv. J. Law & Tec 199, 13958 words, NOTE: PRIVACY AND THE MODERN GRID, Sonia K. McNeil\*

274. Copyright (c) 2010 by the President and Fellows of Harvard College Harvard Journal of Law & Technology, Spring, 2010, Harvard Journal of Law & Technology, 23 Harv. J. Law & Tec 309, 46308 words, ARTICLE: ALL IN THE FAMILY: PRIVACY AND DNA FAMILIAL SEARCHING, Sonia M. Suter\*

275. Copyright (c) 2012 Lewis & Clark Law School Lewis & Clark Law Review, Winter, 2012, Lewis & Clark Law Review, 16 Lewis & Clark L. Rev. 1249, 31529 words, ARTICLE: THE RELATIONAL NATURE OF PRIVACY, by Laurent Sacharoff\*

276. Copyright (c) 2014 President and Fellows of Harvard College Harvard Journal on Legislation, Winter, 2014, Harvard Journal on Legislation, 51 Harv. J. on Legis. 193, 12690 words, NOTE: \*INSTITUTIONALLY APPROPRIATE APPROACHES TO PRIVACY: STRIKING A BALANCE BETWEEN JUDICIAL AND ADMINISTRATIVE ENFORCEMENT OF PRIVACY LAW

277. Copyright (c) 2012 President and Fellows of Harvard College Harvard Journal on Legislation, Winter, 2012, Harvard Journal on Legislation, 49 Harv. J. on Legis. 193, 6819 words, RECENT DEVELOPMENT: TO TRACK OR NOT TO TRACK: RECENT LEGISLATIVE PROPOSALS TO PROTECT CONSUMER PRIVACY, Molly Jennings\*

278. Copyright (c) 2013 Harvard Law Review Association Harvard Law Review, May, 2013, Harvard Law Review, 126 Harv. L. Rev. 1879, 12222 words, SYMPOSIUM: PRIVACY AND TECHNOLOGY: INTRODUCTION: PRIVACY SELF-MANAGEMENT AND THE CONSENT DILEMMA, Daniel J. Solove\*

279. Copyright (c) 2013 Harvard Law Review Association Harvard Law Review, May, 2013, Harvard Law Review, 126 Harv. L. Rev. 1904, 14007 words, SYMPOSIUM: PRIVACY AND TECHNOLOGY: WHAT PRIVACY IS FOR, Julie E. Cohen\*

280. Copyright (c) 2013 Harvard Law Review Association Harvard Law Review, May, 2013, Harvard Law Review, 126 Harv. L. Rev. 1934, 17298 words, SYMPOSIUM: PRIVACY AND TECHNOLOGY: THE DANGERS OF SURVEILLANCE, Neil M. Richards\*

281. Copyright (c) 2013 Harvard Law Review Association Harvard Law Review, May, 2013, Harvard Law Review, 126 Harv. L. Rev. 1966, 24396 words, SYMPOSIUM: PRIVACY AND TECHNOLOGY: THE EU-U.S. PRIVACY COLLISION: A TURN TO INSTITUTIONS AND PROCEDURES, Paul M. Schwartz\*

282. Copyright (c) 2013 Harvard Law Review Association Harvard Law Review, May, 2013, Harvard Law Review, 126 Harv. L. Rev. 2010, 16059 words, SYMPOSIUM: PRIVACY AND TECHNOLOGY: TOWARD A POSITIVE THEORY OF PRIVACY LAW, Lior Jacob Strahilevitz\*

283. Copyright (c) 2011 Harvard Law Review Association Harvard Law Review, November, 2011, Harvard Law Review, 125 Harv. L. Rev. 231, 6704 words, THE SUPREME COURT 2010 TERM: LEADING CASES: I. Constitutional Law: B. Fourth Amendment: Right to Informational Privacy, NASA v. Nelson

284. Copyright (c) 2012 President and Fellows of Harvard College Harvard Law & Policy Review, Symposium, Summer, 2012, Harvard Law & Policy Review, 6 Harv. L. & Pol'y Rev. 263, 5581 words, SYMPOSIUM: PRIVACY AND ACCOUNTABILITY IN THE 21ST CENTURY: Foreword, Nancy Libin \*

285. Copyright (c) 2012 President and Fellows of Harvard College Harvard Law & Policy Review, Symposium, Summer, 2012, Harvard Law & Policy Review, 6 Harv. L. & Pol'y Rev. 273, 10506 words, SYMPOSIUM: PRIVACY AND ACCOUNTABILITY IN THE 21ST CENTURY: Behavioral Advertising: The Offer You Cannot Refuse, Chris Jay Hoofnagle, n1 Ashkan Soltani, n2 Nathaniel Good, n3 Dietrich J. Wambach, n4 and Mika D. Ayenson n5 n6

286. Copyright (c) 2012 President and Fellows of Harvard College Harvard Law & Policy Review, Symposium, Summer, 2012, Harvard Law & Policy Review, 6 Harv. L. & Pol'y Rev. 297, 9958 words, SYMPOSIUM: PRIVACY AND ACCOUNTABILITY IN THE 21ST CENTURY: Fading Privacy Rights of Public Employees, Dieter C. Dammeier \*

287. Copyright (c) 2012 President and Fellows of Harvard College Harvard Law & Policy Review, Symposium, Summer, 2012, Harvard Law & Policy Review, 6 Harv. L. & Pol'y Rev. 313, 10410 words, SYMPOSIUM: PRIVACY AND ACCOUNTABILITY IN THE 21ST CENTURY: Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket, Stephen Wm. Smith \*

288. Copyright (c) 2014 UC Hastings College of the Law Hastings Communications and Entertainment Law Journal (Comm/Ent), Summer, 2014, Hastings Communications and Entertainment Law Journal (Comm/Ent), 36 Hastings Comm. & Ent. L.J. 471, 10473 words, NOTE: Rethinking Online Privacy Litigation as Google Expands Use of Tracking: Giving Meaning to Our Online Browsing and the Federal Wiretap Act, by Filip Babic\*

289. Copyright (c) 2012 UC Hastings College of the Law Hastings Communications and Entertainment Law Journal (Comm/Ent), Fall, 2012, Hastings Communications and Entertainment Law Journal (Comm/Ent), 35 Hastings Comm. & Ent. L.J. 199, 12422 words, NOTE: "I Agreed to What?": A Call for Enforcement of Clarity in the Presentation of Privacy Policies, by DAVID THOMPSON \*

290. Copyright (c) 2011 UC Hastings College of the Law Hastings Communications and Entertainment Law Journal (Comm/Ent), Fall, 2011, Hastings Communications and Entertainment Law Journal (Comm/Ent), 34 Hastings Comm. & Ent. L.J. 127, 9708 words, NOTE: Effective Reader Privacy for Electronic Books: A Proposal, by Jennifer Elmore\*

291. Copyright (c) 2012 UC Hastings College of the Law Hastings Communications and Entertainment Law Journal (Comm/Ent), Spring, 2012, Hastings Communications and Entertainment Law Journal (Comm/Ent), 34 Hastings Comm. & Ent. L.J. 363, 7794 words, COMMENT: Privacy in Social Media: The Right of Publicity, by S. Michael Kernan\*

292. Copyright (c) 2011 UC Hastings College of the Law Hastings Communications and Entertainment Law Journal (Comm/Ent), Spring, 2011, Hastings Communications and Entertainment Law Journal (Comm/Ent), 33 Hastings Comm. & Ent. L.J. 379, 14017 words, ARTICLE: More SPEECH: Preempting Privacy Tourism, by Stephen Bates\*

293. Copyright (c) 2010 UC Hastings College of the Law Hastings Communications and Entertainment Law Journal (Comm/Ent), Spring, 2010, Hastings and Communications Entertainment Law Journal (Comm/Ent), 32 Hastings Comm. & Ent. L.J. 365, 19463 words, ARTICLE: Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages, by Sarah Salter

294. Copyright (c) 2010 UC Hastings College of the Law Hastings Communications and Entertainment Law Journal (Comm/Ent), Spring, 2010, Hastings and Communications Entertainment Law Journal (Comm/Ent), 32 Hastings Comm. & Ent. L.J. 427, 9962 words, NOTE: Cutting Cupid Out of the Workplace: The Capacity of Employees' Constitutional Privacy Rights to Constrain Employers' Attempts to Limit Off-Duty Intimate Associations, by Anna C. Camp

295. Copyright (c) 2014 UC-Hastings College of the Law Hastings Constitutional Law Quarterly, Spring, 2014, Hastings Constitutional Law Quarterly, 41 Hastings Const. L.Q. 649, 16052 words, NOTE: Passwords Please: Rethinking the Constitutional Right to Informational Privacy in the Context of Social Media, by Sara E. Stratton\*

296. Copyright (c) 2014 UC-Hastings College of the Law Hastings Constitutional Law Quarterly, Summer, 2014, Hastings Constitutional Law Quarterly, 41 Hastings Const. L.Q. 875, 11841 words, SYMPOSIUM ARTICLE: On War and Peace in Cyberspace - Security, Privacy, Jurisdiction-, by Lothar Determann\* and Karl T. Guttenberg\*\*

297. Copyright (c) 2014 UC-Hastings College of the Law Hastings Constitutional Law Quarterly, Winter, 2014, Hastings Constitutional Law Quarterly, 41 Hastings Const. L.Q. 357, 11406 words, ARTICLE: Dog Sniffs, Technology, and the Mythical Constitutional Right to Criminal Privacy, by Kenneth J. Melilli\*

298. Copyright (c) 2012 UC-Hastings College of the Law Hastings Constitutional Law Quarterly, Fall, 2012, Hastings Constitutional Law Quarterly, 40 Hastings Const. L.Q. 145, 19022 words, NOTE: Herding Katz: GPS Tracking and Society's Expectations of Privacy in the 21st Century, by Zachary Gray\*

... attempt to determine how society views the extent of its own **privacy** rights in the 21st century, this note uses survey ...

... GPS tracking devices indeed violates reasonable expectations of **privacy.** More importantly, this note argues that the inconsistencies plaguing federal ...

299. Copyright (c) 2013 UC-Hastings College of the Law Hastings Constitutional Law Quarterly, Spring, 2013, Hastings Constitutional Law Quarterly, 40 Hastings Const. L.Q. 475, 23923 words, ARTICLE: A Familial Privacy Right Over Death Images: Critiquing the Internet-Propelled Emergence of a Nascent Constitutional Right that Preserves Happy Memories and Emotions, by Clay Calvert\*

300. Copyright (c) 2013 UC-Hastings College of the Law Hastings Constitutional Law Quarterly, Summer, 2013, Hastings Constitutional Law Quarterly, 40 Hastings Const. L.Q. 925, 21533 words, NOTE: A Check-in on Privacy After United States v. Jones: Current Fourth Amendment Jurisprudence in the Context of Location-Based Applications and Services, by Kathryn Nobuko Horwath\*

301. Copyright (c) 2012 UC-Hastings College of the Law Hastings Constitutional Law Quarterly, Spring, 2012, Hastings Constitutional Law Quarterly, 39 Hastings Const. L.Q. 739, 12273 words, NOTE: Media Liability for Incitement and True Threats under California Abortion Provider Privacy Law, by Aditi Mukherji\*

302. Copyright (c) 2013 UC Hastings College of the Law Hastings International and Comparative Law Review, Winter, 2013, Hastings International and Comparative Law Review, 36 Hastings Int'l & Comp. L. Rev. 257, 13731 words, NOTE: U.S. Preservation Requirements and EU Data Protection: Headed For Collision?, By Tania Abbas\*

... hoard data,European regulators are stepping up enforcement of **privacy** laws that require the systematic elimination of data that identifies individuals ...

... judges can and do order production of evidence despite foreign **privacy** laws forbidding it ? creating a Hobson's choice between ...

... compliance with discovery orders or sanctions abroad for violation of the **privacy** law. But, the ways in which preservation alone can ...

303. Copyright (c) 2011 UC Hastings College of the Law Hastings International and Comparative Law Review, Winter, 2011, Hastings International and Comparative Law Review, 34 Hastings Int'l & Comp. L. Rev. 177, 12765 words, NOTE: Electronic Medical Records and the Challenge to Privacy: How the United States and Canada Are Responding, By Elana Rivkin-Haas\*

304. Copyright (c) 2010 U.C. Hastings College of the Law Hastings Law Journal, December, 2010, Hastings Law Journal, 62 Hastings L.J. 357, 23142 words, ARTICLE: Stanley in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like That of the Fourth, Marc Jonathan Blitz\*

305. Copyright (c) 2011 U.C. Hastings College of the Law Hastings Law Journal, February, 2011, Hastings Law Journal, 62 Hastings L.J. 795, 12853 words, Note: Don't Steal My Sunshine: Deconstructing the Flawed Presumption of Privacy for Unfiled Documents Exchanged During Discovery, Mary Elizabeth Keaney\*

306. Copyright (c) 2011 U.C. Hastings College of the Law Hastings Law Journal, March, 2011, Hastings Law Journal, 62 Hastings L.J. 1037, 14274 words, Note: Privacy and Security During Life, Access After Death: Are They Mutually Exclusive?, Molly Wilkens\*

307. Copyright © 2010 University of California, Hastings College of the Law. All Rights Reserved. Hastings Science & Technology Law Journal, Summer, 2010, Hasting Journal of Science & Technology Law Journal, 2 Hastings Sci. & Tech. L.J. 137, 19028 words, ARTICLE: Search Query Privacy: The Problem of Anonymization, by RON A. DOLIN, J.D., PH.D. \*

308. Copyright (c) 2011 University of Hawai'i Law Review University of Hawai'i Law Review, Summer, 2011, University of Hawai'i Law Review, 33 Hawaii L. Rev. 669, 21392 words, SYMPOSIUM ISSUE: THE MOON COURT ERA: Hawai'i's Right to Privacy, Jon M. Van Dyke\* and Melissa Uhl\*\*

309. Copyright (c) 2010 University of Hawai'i Law Review University of Hawai'i Law Review, Summer, 2010, University of Hawaii Law Review, 32 Hawaii L. Rev. 305, 9578 words, ARTICLE: The Privacy Rights of Public School Students, Jon M. Van Dyke\*

310. Copyright (c) 2014 Case Western Reserve University Health Matrix: Journal of Law-Medicine, 2014, Health Matrix: Journal of Law Medicine, 24 Health Matrix 11, 16774 words, SYMPOSIUM: SUSTAINABLE ACCESS TO DATA FOR POSTMARKETING MEDICAL PRODUCT SAFETY SURVEILLANCE UNDER THE AMENDED HIPAA PRIVACY RULE, Barbara J. Evans +

311. Copyright (c) 2014 Case Western Reserve University Health Matrix: Journal of Law-Medicine, 2014, Health Matrix: Journal of Law Medicine, 24 Health Matrix 49, 7301 words, SYMPOSIUM: PRIVACY VS. PROGRESS: RESEARCH EXCEPTIONALISM IS BAD MEDICINE, Suzanne M. Rivera +

312. Copyright (c) 2014 Case Western Reserve University Health Matrix: Journal of Law-Medicine, 2014, Health Matrix: Journal of Law Medicine, 24 Health Matrix 65, 20808 words, SYMPOSIUM: Big Data Proxies and Health Privacy Exceptionalism \*, Nicolas P. Terry+

313. Copyright (c) 2013 Case Western Reserve University Health Matrix: Journal of Law-Medicine, 2013, Health Matrix: Journal of Law Medicine, 22 Health Matrix 489, 21488 words, ARTICLE: PROTECTION FOR PSYCHOTHERAPY NOTES UNDER THE HIPAA PRIVACY RULE: AS PRIVATE AS A HOSPITAL GOWN n1, Stephanie O. Corley+

314. Copyright (c) 2011 Hofstra Law Review Association Hofstra Law Review, Winter, 2011, Hofstra Law Review, 40 Hofstra L. Rev. 473, 24753 words, NOTE: WHO IS POKING AROUND YOUR FACEBOOK PROFILE?: THE NEED TO REFORM THE STORED COMMUNICATIONS ACT TO REFLECT A LACK OF PRIVACY ON SOCIAL NETWORKING WEBSITES, Lindsay S. Feuer\*

315. Copyright (c) 2012 Hofstra Law Review Association Hofstra Law Review, Spring, 2012, Hofstra Law Review, 40 Hofstra L. Rev. 811, 22269 words, NOTE: LOOK OVER YOUR FIGURATIVE SHOULDER: HOW TO SAVE INDIVIDUAL DIGNITY AND PRIVACY ON THE INTERNET, Maayan Y. Vodovis\*

316. Copyright (c) 2012 Houston Business & Tax Law Journal Houston Business & Tax Law Journal, 2012, Houston Business and Tax Law Journal, 12 Hous. Bus. & Tax L.J. 194, 15671 words, ARTICLE: TRANSPARENCY V. INTELLIGENCE: CORPORATE INFORMATION PRIVACY RIGHTS UNDER THE FREEDOM OF INFORMATION ACT AND WHETHER INQUIRING MINDS STILL HAVE A RIGHT TO KNOW, Nicole Washington

317. Copyright (c) 2010 Houston Law Review Houston Law Review, Winter, 2010, HOUSTON LAW REVIEW, 46 Hous. L. Rev. 1545, 28877 words, ARTICLE: THE CELEBRITY CEO: CORPORATE DISCLOSURE AT THE INTERSECTION OF PRIVACY AND SECURITIES LAW, Patricia Sanchez Abril\* and Ann M. Olazabal\*\*

318. Copyright (c) 2012 Howard University School of Law Howard Law Journal, Fall, 2012, Howard Law Journal, 56 How. L.J. 169, 16838 words, ARTICLE: Mean Girls and Boys: The Intersection of Cyberbullying and Privacy Law and Its Social-Political Implications, Nicole P. Grant\*

319. Copyright (c) 2013 Howard University School of Law Howard Law Journal, Spring, 2013, Howard Law Journal, 56 How. L.J. 951, 14322 words, NINTH ANNUAL WILEY A. BRANTON/HOWARD LAW JOURNAL SYMPOSIUM: Protest & Polarization: Law and Debate in America 2012: Note & Comment: Fundamental Right or Liberty?: Online Privacy's Theory for Co-Existence with Social Media, Hakeem Rizk\*

320. Copyright (c) 2011 Howard University School of Law Howard Law Journal, Fall, 2011, Howard Law Journal, 55 How. L.J. 205, 21824 words, NOTE & COMMENT: Keep the Court Room Doors Closed So the Doors of Opportunity Can Remain Open: An Argument for Maintaining Privacy in the Juvenile Justice System, Leila R. Siddiky\*

321. Copyright (c) 2010 The Board of Trustees of the University of Illinois University of Illinois Journal of Law, Technology & Policy, Spring, 2010, University of Illinois Journal of Law, Technology & Policy, 2010 U. Ill. J.L. Tech. & Pol'y 1, 28600 words, ARTICLE: PRIVACY INVASIVE GEO-MASHUPS: PRIVACY 2.0 AND THE LIMITS OF FIRST GENERATION INFORMATION PRIVACY LAWS, Mark Burdon+

322. Copyright (c) 2010 The Board of Trustees of the University of Illinois University of Illinois Journal of Law, Technology & Policy, Spring, 2010, University of Illinois Journal of Law, Technology & Policy, 2010 U. Ill. J.L. Tech. & Pol'y 157, 15573 words, NOTE: PRIVACY AT A PRICE: DIRECT-TO-CONSUMER GENETIC TESTING & THE NEED FOR REGULATION, Molly C. Novy\*

323. Copyright (c) 2014 The Board of Trustees of the University of Illinois University of Illinois Journal of Law, Technology & Policy, Spring, 2014, University of Illinois Journal of Law, Technology & Policy, 14 U. Ill. J.L. Tech. & Pol'y 1, 32690 words, ARTICLE: THE REVOLUTION WILL BE TWEETED, BUT THE TWEETS WILL BE SUBPOENAED: REIMAGINING FOURTH AMENDMENT PRIVACY TO PROTECT ASSOCIATIONAL ANONYMITY, Chris J. Chasin+

324. Copyright (c) 2014 The Board of Trustees of the University of Illinois University of Illinois Journal of Law, Technology & Policy, Spring, 2014, University of Illinois Journal of Law, Technology & Policy, 14 U. Ill. J.L. Tech. & Pol'y 177, 13694 words, ESSAY: FEDERATED IDENTITY MANAGEMENT AND THE NSTIC: CO-MANAGING INFORMATION PRIVACY, Amanda Craig+

325. Copyright (c) 2014 The Board of Trustees of the University of Illinois University of Illinois Journal of Law, Technology & Policy, Spring, 2014, University of Illinois Journal of Law, Technology & Policy, 14 U. Ill. J.L. Tech. & Pol'y 283, 14169 words, NOTE: TAKING MATTERS INTO ITS OWN HANDS: WHY CONGRESS SHOULD PASS LEGISLATION TO ALLOW THE FTC TO REGULATE CONSUMER ONLINE PRIVACY WITH A "DO NOT TRACK" MECHANISM, Angelica Nizio\*

326. Copyright (c) 2013 The Board of Trustees of the University of Illinois University of Illinois Law Review, 2013, University of Illinois Law Review, 2013 U. Ill. L. Rev. 625, 23463 words, NOTE: PROSTITUTION AND THE RIGHT TO PRIVACY: A COMPARATIVE ANALYSIS OF CURRENT LAW IN THE UNITED STATES AND CANADA, Dannia Altemimei\*

327. Copyright (c) 2010 Trustees of Indiana University Indiana International & Comparative Law Review, 2010, Indiana International & Comparative Law Review, 20 Ind. Int'l & Comp. L. Rev. 21, 12753 words, ARTICLE: In Search of a New Approach of Information Privacy Judicial Review: Interpretation No. 603 of Taiwan's Constitutional Court as a Guide, Chung-Lin Chen\*

328. Copyright (c) 2013 Trustees of Indiana University Indiana Law Journal, Winter, 2013, Indiana Law Journal, 88 Ind. L.J. 361, 19308 words, NOTE: Balancing the Scales: Reinstating Home Privacy Without Violence in Indiana, Tyler Anderson\*

329. Copyright (c) 2013 Trustees of Indiana University Indiana Law Journal, Summer, 2013, Indiana Law Journal, 88 Ind. L.J. 881, 18246 words, ARTICLE: The Polysemy of Privacy, Ronald J. Krotoszynski, Jr.\*

330. Copyright (c) 2013 Trustees of Indiana University Indiana Law Journal, Fall, 2013, Indiana Law Journal, 88 Ind. L.J. 1593, 13948 words, Note: A New Approach to Digital Reader Privacy: State Regulations and Their Protection of Digital Book Data, Andrew A. Proia\*

331. Copyright (c) 2011 Trustees of Indiana University Indiana Law Journal, Summer, 2011, Indiana Law Journal, 86 Ind. L.J. 1131, 16119 words, ESSAY: The Boundaries of Privacy Harm, M. Ryan Calo\*

332. Copyright (c) 2013 The Trustees of Indiana University Indiana Law Review, 2013, Indiana Law Review, 46 Ind. L. Rev. 311, 15141 words, ARTICLE: Plotting Privacy as Intimacy, Heidi Reamer Anderson\*

333. Copyright (c) 2014 Intercultural Human Rights Law Review, All Rights Reserved. Intercultural Human Rights Law Review, 2013, Intercultural Human Rights Law Review, 8 Intercultural Hum. Rts. L. Rev. 177, 19197 words, ARTICLE: PRIVACY-INVADING TECHNOLOGIES AND RECOMMENDATIONS FOR DESIGNING A BETTER FUTURE FOR PRIVACY RIGHTS, ALEXANDRA RENGEL \*

334. Copyright (c) 2011 The University of Iowa Iowa Law Review, November, 2011, Iowa Law Review, 97 Iowa L. Rev. 303, 9971 words, NOTE: Keep Closed Containers Closed: Resolving the Circuit Split in Favor of Individual Privacy, Brian D. Jones\*

335. Copyright (c) 2012 The University of Iowa Iowa Law Review, January, 2012, Iowa Law Review, 97 Iowa L. Rev. 665, 13611 words, NOTE: Privacy for Safety: The NCAA Sickle-Cell Trait Testing Policy and the Potential for Future Discrimination, Heather R. Quick\*

336. Copyright (c) 2012 The University of Iowa Iowa Law Review, March, 2012, Iowa Law Review, 97 Iowa L. Rev. 809, 14941 words, ARTICLE: Self-Surveillance Privacy, Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke, and Mark Hansen\*

337. Copyright (c) 2012 The University of Iowa Iowa Law Review, May, 2012, Iowa Law Review, 97 Iowa L. Rev. 1283, 9861 words, NOTE: Safe for Work? Analyzing the Supreme Court's Standard of Privacy for Government Employees in Light of City of Ontario v. Quon, Sheila A. Bentzen\*

338. Copyright (c) 2010 The University of Iowa Iowa Law Review, February, 2010, IOWA LAW REVIEW, 95 Iowa L. Rev. 631, 14163 words, Article: Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records, Mark A. Hall\*

339. Copyright (c) 2010 The University of Iowa Iowa Law Review, March, 2010, Iowa Law Review, 95 Iowa L. Rev. 919, 27606 words, ARTICLE: "We, the Paparazzi": Developing a Privacy Paradigm for Digital Video, Jacqueline D. Lipton\*

340. Copyright (c) 2012 Israel Law Review Israel Law Review, November, 2012, Israel Law Review, 45 Isr. L. Rev. 537, 10432 words, ARTICLE: SEX, SCANDAL AND SUPER-INJUNCTIONS -- THE CONTROVERSIES SURROUNDING THE PROTECTION OF PRIVACY, Lord Anthony Grabiner QC \*

341. Copyright (c) 2011 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall, 2011, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 75, 14747 words, 2012 JOHN MARSHALL INTERNATIONAL MOOT COURT COMPETITION IN INFORMATION TECHNOLOGY AND PRIVACY LAW: BENCH MEMORANDUM, Russell Bottom, Matthew T. Andris and Robin Ann Sowizrol

342. Copyright (c) 2011 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall, 2011, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 103, 16683 words, 2012 JOHN MARSHALL LAW SCHOOL INTERNATIONAL MOOT COURT COMPETITON IN INFORMATION TECHNOLOGY AND PRIVACY LAW: BRIEF FOR THE PETITIONER, Nate Lindsey and Chris Omlid

343. Copyright (c) 2011 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall, 2011, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 139, 12263 words, 2012 JOHN MARSHALL LAW SCHOOL INTERNATIONAL MOOT COURT COMPETITON IN INFORMATION TECHNOLOGY AND PRIVACY LAW: BRIEF FOR THE RESPONDENT

344. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Spring / Summer, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 279, 1831 words, THE 20TH BELLE R. AND JOSEPH H. BRAUN MEMORIAL SYMPOSIUM: THE DEVELOPMENT OF PRIVACY LAW FROM BRANDEIS TO TODAY: OPENING REMARKS

345. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Spring / Summer, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 285, 14467 words, THE 20TH BELLE R. AND JOSEPH H. BRAUN MEMORIAL SYMPOSIUM: THE DEVELOPMENT OF PRIVACY LAW FROM BRANDEIS TO TODAY: SESSION I: THE LEGACY OF JUSTICE ARTHUR GOLDBERG, Moderator: Samuel R. Olken Professor, The John Marshall Law School Panelists: Gerald Berendt Professor, The John Marshall Law School Gilbert A. Cornfield Cornfield and Feldman Gilbert Feldman Cornfield and Feldman Hon. Milton I. Shadur Senior Judge, U.S. District Court for the Northern District of Illinois, Eastern Division Dr. David Stebenne Professor, The Ohio State University

346. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Spring / Summer, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 319, 10108 words, THE 20TH BELLE R. AND JOSEPH H. BRAUN MEMORIAL SYMPOSIUM: THE DEVELOPMENT OF PRIVACY LAW FROM BRANDEIS TO TODAY: SESSION II: HISTORICAL PERSPECTIVES ON PRIVACY IN AMERICAN LAW, Moderator: Steven D. Schwinn Associate Professor, The John Marshal Law School Panelists: Alberto Bernabe Professor, The John Marshall Law School Kathryn Kolbert Constance Hess Williams Director of the Athena Center for Leadership Studies, Barnard College Dr. Adam D. Moore Associate Professor, University of Washington Marc Rotenberg Executive Director, Electronic Privacy Information Center

347. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Spring / Summer, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 343, 15410 words, THE 20TH BELLE R. AND JOSEPH H. BRAUN MEMORIAL SYMPOSIUM: THE DEVELOPMENT OF PRIVACY LAW FROM BRANDEIS TO TODAY: SESSION III: PRIVACY REGULATION AND POLICY PERSPECTIVES, Moderator: Leslie Ann Reis Assistant Professor; Director, Center for Information Technology and Privacy Law, The John Marshall Law School Panelists: Mary Ellen Callahan Jenner & Block Renard Francois Corporate Counsel, Caterpillar Financial Services Corp. Peter P. Swire C. William O'Neill Professor in Law and Judicial Administration, The Ohio State University Moritz College of Law

348. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Spring / Summer, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 379, 10659 words, THE 20TH BELLE R. AND JOSEPH H. BRAUN MEMORIAL SYMPOSIUM: THE DEVELOPMENT OF PRIVACY LAW FROM BRANDEIS TO TODAY: SESSION IV: TECHNOLOGY AND THE FUTURE OF PRIVACY, Moderator: David E. Sorkin Associate Professor, The John Marshall Law School Panelists: Anne Bartow Professor, Pace University School of Law Robert S. Gurwin Assistant General Counsel, AOL Inc. Doris Estelle Long Professor, The John Marshall Law School

349. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Spring / Summer, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 405, 4752 words, THE 20TH BELLE R. AND JOSEPH H. BRAUN MEMORIAL SYMPOSIUM: THE DEVELOPMENT OF PRIVACY LAW FROM BRANDEIS TO TODAY: DEDICATION OF THE ARTHUR J. GOLDBERG MEMORIAL COURTROOM: FRIDAY, SEPTEMBER 28, 2012, Hon. Antonin Scalia

350. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Spring / Summer, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 419, 20435 words, ARTICLE: A LIBERAL COMMUNITARIAN CONCEPTION OF PRIVACY, Amitai Etzioni\*

351. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Spring / Summer, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 463, 13293 words, ARTICLE: DRUG TESTING AND PRIVACY IN THE WORKPLACE, Adam D. Moore\*

352. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Spring / Summer, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 493, 9428 words, ARTICLE: GIVING CREDIT WHERE CREDIT IS DUE: A COMMENT ON THE THEORETICAL FOUNDATION AND HISTORICAL ORIGIN OF THE TORT REMEDY FOR INVASION OF PRIVACY, Alberto Bernabe\*

353. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall / Winter, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 637, 23589 words, COMMENT: WHAT'S MINE IS YOURS: TARGETING PRIVACY ISSUES AND DETERMINING THE BEST SOLUTIONS FOR BEHAVIORAL ADVERTISING, Sarah Cathryn Brandon n1

354. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall / Winter, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 673, 14700 words, 2012 JOHN MARSHALL LAW SCHOOL INTERNATIONAL MOOT COURT COMPETITION IN INFORMATION TECHNOLOGY AND PRIVACY LAW: BENCH MEMORANDUM, Russell Bottom, Greer Herman, Catherine Nance, Robin Ann Sowizrol and Gina Spada

355. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall / Winter, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 701, 13711 words, 2012 JOHN MARSHALL LAW SCHOOL INTERNATIONAL MOOT COURT COMPETITION IN INFORMATION TECHNOLOGY AND PRIVACY LAW: BRIEF FOR PETITIONER, Kyle Fonville, Grace Hwang and Nivesh Oudit

356. Copyright (c) 2012 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall / Winter, 2012, The John Marshall Journal of Computer & Information Law, 29 J. Marshall J. Computer & Info. L. 733, 14360 words, 2012 JOHN MARSHALL LAW SCHOOL INTERNATIONAL MOOT COURT COMPETITION IN INFORMATION TECHNOLOGY AND PRIVACY LAW: BRIEF FOR RESPONDENT, Christopher Dabney and Kara Frankman

357. Copyright (c) 2010 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall, 2010, The John Marshall Journal of Computer & Information Law, 28 J. Marshall J. Computer & Info. L. 49, 16588 words, COMMENT: THE OLYMPIC MEDDLE: THE INTERNATIONAL OLYMPIC COMMITTEE'S INTRUSION OF ATHLETES' PRIVACY THROUGH THE DISCRIMINATORY PRACTICE OF GENDER VERIFICATION TESTING, By: Raheel Saleem\*

358. Copyright (c) 2010 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall, 2010, The John Marshall Journal of Computer & Information Law, 28 J. Marshall J. Computer & Info. L. 81, 21396 words, 2010 JOHN MARSHALL LAW SCHOOL INTERNATIONAL MOOT COURT COMPETITION IN INFORMATION TECHNOLOGY AND PRIVACY LAW: THE TWENTY-NINTH ANNUAL JOHN MARSHALL INTERNATIONAL MOOT COURT COMPETITION IN INFORMATION TECHNOLOGY AND PRIVACY LAW OCTOBER 28-30, 2010: BENCH MEMORANDUM, Erin Murphy-Hillstrom, Whitney Hutchinson, Efthymios Katsarelis, Amber Lynn Wagner and Panagiota Kelali

359. Copyright (c) 2010 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall, 2010, The John Marshall Journal of Computer & Information Law, 28 J. Marshall J. Computer & Info. L. 119, 13885 words, 2010 JOHN MARSHALL LAW SCHOOL INTERNATIONAL MOOT COURT COMPETITION IN INFORMATION TECHNOLOGY AND PRIVACY LAW: BRIEF FOR PETITIONER, AARON MURPHY, Petitioner, v. MARSHCODE CORPORATION, Respondent., Kelly Foss, Vince Lombardozzi and Jared Palmer

360. Copyright (c) 2010 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Fall, 2010, The John Marshall Journal of Computer & Information Law, 28 J. Marshall J. Computer & Info. L. 151, 15388 words, 2010 JOHN MARSHALL LAW SCHOOL INTERNATIONAL MOOT COURT COMPETITION IN INFORMATION TECHNOLOGY AND PRIVACY LAW: BRIEF FOR RESPONDENT, AARON MURPHY, Petitioner, v. MARSHCODE CORP., a Marshall Corporation, Respondent., Kimberly Hodgman, Jody Rodenberg and Erin Tyler

361. Copyright (c) 2011 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Summer, 2011, The John Marshall Journal of Computer & Information Law, 28 J. Marshall J. Computer & Info. L. 551, 18501 words, COMMENT: CARRY THAT WEIGHT: VICTIM PRIVACY WITHIN THE MILITARY SEXUAL ASSAULT REPORTING METHODS, Emily Hansen\*

362. Copyright (c) 2010 The John Marshall Law School The John Marshall Journal of Computer & Information Law, Summer, 2010, The John Marshall Journal of Computer and Information Law, 27 J. Marshall J. Computer & Info. L. 593, 8879 words, ARTICLE: AN EVOLUTIONARY STUDY OF CLOUD COMPUTING SERVICES PRIVACY TERMS, Konstantinos K. Stylianou\*

363. Copyright (c) 2012 The John Marshall Law School The John Marshall Law Review, Fall, 2012, John Marshall Law Review, 46 J. Marshall L. Rev. 309, 9623 words, COMMENT: WHERE ART THOU, PRIVACY?: EXPANDING PRIVACY RIGHTS OF MINORS IN REGARD TO CONSENSUAL SEX: STATUTORY RAPE LAWS AND THE NEED FOR A "ROMEO AND JULIET" EXCEPTION IN ILLINOIS, Jordan Franklin\*

364. Copyright (c) 2011 The John Marshall Law School The John Marshall Law Review, Fall, 2011, John Marshall Law Review, 45 J. Marshall L. Rev. 1, 9899 words, ARTICLE: FOLLOWING YOU HERE, THERE, AND EVERYWHERE: AN INVESTIGATION OF GPS TECHNOLOGY, PRIVACY, AND THE FOURTH AMENDMENT, Stephanie G. Forbes\*

365. Copyright (c) 2011 The John Marshall Law School The John Marshall Law Review, Fall, 2011, John Marshall Law Review, 45 J. Marshall L. Rev. 175, 11285 words, COMMENT: REVISITING READER PRIVACY IN THE AGE OF THE E-BOOK, Bradley Schaufenbuel\*

366. Copyright (c) 2013 The John Marshall Law School The John Marshall Law School Review of Intellectual Property Law, Special, 2013, The John Marshall Law School Review of Intellectual Property Law, 12 J. Marshall Rev. Intell. Prop. L. 551, 16053 words, ARTICLE: THE EMERGING REALITY OF SOCIAL MEDIA: EROSION OF INDIVIDUAL PRIVACY THROUGH CYBER-VETTING AND LAW'S INABILITY TO CATCH UP, DR. SABY GHOSHRAY \*

367. Copyright (c) 2013 Southern Methodist University Dedman School of Law Journal of Air Law and Commerce, Summer, 2013, Journal of Air Law & Commerce, 78 J. Air L. & Com. 617, 17364 words, COMMENT: THE TSA'S NEW PRECHECK IS BEGINNING TO LOOK A LOT LIKE CAPPS II: THE PRIVACY IMPLICATIONS OF REVIVING THE TENETS OF THE FAILED PREDECESSOR, Katie Cristina\*

368. Copyright (c) 2013 Southern Methodist University Dedman School of Law Journal of Air Law and Commerce, Fall, 2013, Journal of Air Law & Commerce, 78 J. Air L. & Com. 711, 12914 words, ARTICLE: THE D.C. CIRCUIT'S EPIC FAILURE IN ELECTRONIC PRIVACY INFORMATION CENTER V. UNITED STATES DEPARTMENT OF HOMELAND SECURITY, R. Gregory Israelsen\*

369. Copyright (c) 2012 Southern Methodist University Dedman School of Law Journal of Air Law and Commerce, Summer, 2012, Journal of Air Law & Commerce, 77 J. Air L. & Com. 439, 11730 words, ARTICLE: UNMANNED BUT ACCELERATING: NAVIGATING THE REGULATORY AND PRIVACY CHALLENGES OF INTRODUCING UNMANNED AIRCRAFT INTO THE NATIONAL AIRSPACE SYSTEM, Benjamin Kapnik\*

370. Copyright (c) 2012 Southern Methodist University Dedman School of Law Journal of Air Law and Commerce, Summer, 2012, Journal of Air Law & Commerce, 77 J. Air L. & Com. 569, 20321 words, COMMENT: MAINTAINING PRIVACY IN A WORLD OF TECHNOLOGICAL TRANSPARENCY? THE BARR PROGRAM'S UPS AND DOWNS IN CHANGING TIMES, Olga Gurtovaya\*

371. Copyright (c) 2010 American Academy of Matrimonial Lawyers Journal of the American Academy of Matrimonial Lawyers, 2010, Journal of the American Academy of Matrimonial Lawyers, 23 J. Am. Acad. Matrimonial Law. 99, 4353 words, ELECTRONIC EVIDENCE: Article: Privacy and Litigation: Two Mutually Exclusive Concepts, By Hon. Margaret Dee McGarity+

372. Copyright (c) 2010 American Academy of Matrimonial Lawyers Journal of the American Academy of Matrimonial Lawyers, 2010, Journal of the American Academy of Matrimonial Lawyers, 23 J. Am. Acad. Matrimonial Law. 111, 7276 words, ELECTRONIC EVIDENCE: Article: The Individual's Right of Privacy in a Marriage, by Laura W. Morgan\* and Lewis B. Reich\*\*

373. Copyright (c) 2011 St. John's University Journal of Civil Rights and Economic Development, Summer, 2011, Journal of Civil Rights and Economic Development, 25 J. Civ. Rts. & Econ. Dev. 833, 18142 words, NOTE: THE PRIVACY OF DEATH ON THE INTERNET: A LEGITIMATE MATTER OF PUBLIC CONCERN OR MORBID CURIOSITY, David Hamill\*

374. Copyright (c) 2012 The Catholic University of America Journal of Contemporary Health Law & Policy, Spring, 2012, Journal of Contemporary Health Law & Policy, 28 J. Contemp. Health L. & Pol'y 324, 12175 words, COMMENT: MEDICATION ADHERENCE TECHNOLOGY: MEDICINE OF THE FUTURE, EMERGING PRIVACY CONCERN, Katherine Boshinski Sparks \*

375. Copyright (c) 2013 Northwestern University, School of Law Journal of Criminal Law & Criminology, Summer, 2013, Journal of Criminal Law & Criminology, 103 J. Crim. L. & Criminology 667, 8827 words, SYMPOSIUM ON CYBERCRIME: PRIVACY VERSUS SECURITY, DEREK E. BAMBAUER\*

376. Copyright (c) 2013 Northwestern University, School of Law Journal of Criminal Law & Criminology, Summer, 2013, Journal of Criminal Law & Criminology, 103 J. Crim. L. & Criminology 985, 15491 words, COMMENT: ADVENTURES ON THE AUTOBAHN AND INFOBAHN: UNITED STATES V. JONES, MANDATORY DATA RETENTION, AND A MORE REASONABLE "REASONABLE EXPECTATION OF PRIVACY", John A. Stratford\*

377. Copyright (c) 2012 Northwestern University, School of Law Journal of Criminal Law & Criminology, Winter, 2012, Journal of Criminal Law & Criminology, 102 J. Crim. L. & Criminology 253, 13565 words, COMMENT: THE DATA-BROKER THREAT: PROPOSING FEDERAL LEGISLATION TO PROTECT POST-EXPUNGEMENT PRIVACY, Logan Danielle Wayne\*

378. Copyright (c) 2014 Journal of High Technology Law Journal of High Technology Law, 2014, Journal of High Technology Law, 14 J. High Tech. L. 120, 10325 words, ARTICLE: PRIVACY PROTECTIONS LEFT WANTING: LOOKING AT DOCTRINE AND SAFEGUARDS ON LAW ENFORCEMENT'S USE OF GPS TRACKING AND CELL PHONE RECORDS WITH A FOCUS ON MASSACHUSETTS, Lloyd Chebaclo \*

379. Copyright (c) 2011 Journal of High Technology Law Journal of High Technology Law, 2011, Journal of High Technology Law, 11 J. High Tech. L. 229, 22783 words, ARTICLE: ON PRIVACY: LIBERTY IN THE DIGITAL REVOLUTION, Christina M. Gagnier \*

380. Copyright (c) 2010 Journal of High Technology Law Journal of High Technology Law, February 2010, Journal of High Technology Law, 10 J. High Tech. L. 4, 303 words, ARTICLE: Tension Between Privacy and Law Enforcement on the Web

381. Copyright (c) 2013 Journal of Intellectual Property Law Association Journal of Intellectual Property Law, Spring, 2013, Journal of Intellectual Property Law, 20 J. Intell. Prop. L. 413, 17846 words, NOTE: JUST YOU AND ME AND NETFLIX MAKES THREE: IMPLICATIONS FOR ALLOWING "FRICTIONLESS SHARING" OF PERSONALLY IDENTIFIABLE INFORMATION UNDER THE VIDEO PRIVACY PROTECTION ACT, Kathryn Elizabeth McCabe\*

382. Copyright (c) 2014 Alberta Law Review Alberta Law Review, March, 2014, Alberta Law Review, 51 Alberta L. Rev. 471, 12968 words, ARTICLE: PRIVACY PROTECTION AND GENETIC RESEARCH: WHERE DOES THE PUBLIC INTEREST LIE?, UBAKA OGBOGU \* AND SARAH BURNINGHAM \*\*

383. Copyright (c) 2010 Alberta Law Review Alberta Law Review, June, 2010, Alberta Law Review, 47 Alberta L. Rev. 1037, 6031 words, CASE COMMENT: DISCARDING REASONABLE EXPECTATIONS OF PRIVACY: A CRITIQUE OF R. V. PATRICK, WILLIAM MACKINNON\*

384. Copyright (c) 2014 Journal of Law, Economics & Policy Journal of Law, Economics & Policy, Spring, 2014, Journal of Law, Economics & Policy, 10 J.L. Econ. & Pol'y 441, 13214 words, Student Comment: An Economic Perspective on the Privacy Implications of Domestic Drone Surveillance, Ian F. Rothfuss\*

385. Copyright (c) 2013 Journal of Law, Economics & Policy Journal of Law, Economics & Policy, Spring, 2013, Journal of Law, Economics & Policy, 9 J.L. Econ. & Pol'y 461, 13219 words, 7th Annual Judicial Symposium on Civil Justice Issues: George Mason Judicial Education Program: Edited Transcripts: The Economics of Privacy and Data Security, Anna H. Davis, Nuala O'Connor, Matthew Fitzsimmons and Lisa J. Sotto Moderator: James C. Cooper

386. Copyright (c) 2011 Journal of Law, Economics & Policy Journal of Law, Economics & Policy, Winter, 2011, Journal of Law, Economics & Policy, 8 J.L. Econ. & Pol'y 301, 16427 words, 6TH ANNUAL JUDICIAL SYMPOSIUM ON CIVIL JUSTICE ISSUES GEORGE MASON JUDICIAL EDUCATION PROGRAM NOVEMBER 13-15, 2011: EDITED TRANSCRIPT: PRIVACY ENFORCEMENT UNDER STATE CONSUMER PROTECTION ACTS, Justin Brookman, Shannon Choy-Seymour, David Lieber, Michael Martone Moderator: James Cooper

387. Copyright (c) 2014 Jefferson Law Book Company Journal of Law & Education, Winter, 2014, Journal of Law & Education, 43 J.L. & Educ. 65, 7265 words, COUNTERPOINT: Customizable "Sexual Orientation Privacy" for Minor Schoolchildren: A Law School Invention in Search of a Constitutional Mandate, Christopher A. Ferrara \*

388. Copyright (c) 2013 Jefferson Law Book Company Journal of Law & Education, Summer, 2013, Journal of Law & Education, 42 J.L. & Educ. 381, 16348 words, ARTICLE: The Right to Sexual Orientation Privacy: Strengthening Protections for Minors Who Are "Outed" in Schools, ADAM J. KRETZ \*

389. Copyright (c) 2011 Jefferson Law Book Company Journal of Law & Education, July, 2011, Journal of Law & Education, 40 J.L. & Educ. 417, 19830 words, ARTICLE: Please Don't Tell My Mom! A Minor's Right to Informational Privacy, CAITLIN M. CULLITAN \*

390. Copyright (c) 2011 Journal of Law & Family Studies Journal of Law & Family Studies, 2011, Journal of Law & Family Studies, 13 J. L. Fam. Stud. 117, 19412 words, ARTICLE: Same-Sex Marriage and the Right to Privacy, Mark Strasser\*

391. Copyright (c) 2011 Journal of Law & Family Studies Journal of Law & Family Studies, 2011, Journal of Law & Family Studies, 13 J. L. Fam. Stud. 345, 9371 words, BOOK NOTE: Jeannie Suk, "At Home in the Law: How the Domestic Violence Revolution Is Transforming Privacy" (2009), Mark Schwarz\*

392. Copyright (c) 2010 Journal of Law & Family Studies Journal of Law & Family Studies, 2010, JOURNAL OF LAW & FAMILY STUDIES, 12 J. L. Fam. Stud. 87, 36676 words, Article: The Huck Finn Syndrome in History and Theory: The Origins of Family Privacy, Steven J. Macias\*

393. Copyright (c) 2013 American Society of Law, Medicine & Ethics Journal of Law, Medicine & Ethics, Summer, 2013, Journal of Law, Medicine and Ethics, 41 J.L. Med. & Ethics 525, 4112 words, COLUMN: HIPAA Privacy Rule 2.0: Currents in Contemporary Bioethics, Mark A. Rothstein

394. Copyright (c) 2011 American Society of Law, Medicine & Ethics Journal of Law, Medicine & Ethics, Summer, 2011, Journal of Law, Medicine and Ethics, 39 J.L. Med. & Ethics 280, 4598 words, COLUMN: Currents in Contemporary Bioethics: Constitutional Right to Informational Health Privacy in Critical Condition, Mark A. Rothstein

395. Copyright (c) 2011 American Society of Law, Medicine & Ethics Journal of Law, Medicine & Ethics, Fall, 2011, Journal of Law, Medicine and Ethics, 39 J.L. Med. & Ethics 469, 17636 words, SYMPOSIUM: Public Health Reform: Patient Protection and Affordable Care Act Implications for the Public's Health: When Public Health and Genetic Privacy Collide: Positive and Normative Theories Explaining How ACA's Expansion of Corporate Wellness Programs Conflicts with GINA's Privacy Rules, Jennifer S. Bard Guest Edited by Elizabeth Weeks Leonard

396. Copyright (c) 2012 University of Florida Journal of Law & Public Policy University of Florida Journal of Law & Public Policy, August, 2012, University of Florida Journal of Law & Public Policy, 23 U. Fla. J.L. & Pub. Pol'y 235, 11264 words, NOTE: IDENTITY, PRIVACY AND CRIME: PRIVACY AND PUBLIC RECORDS IN FLORIDA, Martin A. Holland\*

397. Copyright (c) 2011 Wayne State University The Journal of Law in Society, Fall, 2011, The Journal of Law in Society, 13 J.L. Soc'y 353, 15772 words, NOTE: THE AFTERMATH OF "THE DETROIT CONTROVERSY": EAVESDROPPING ON ACTING PUBLIC OFFICIALS AND THEIR PRIVACY RIGHTS, ERIC TURNBULL n1

398. Copyright (c) 2013 The University of Chicago The Journal of Legal Studies, June, 2013, The Journal of Legal Studies, 42 J. Legal Stud. 249, 10760 words, ARTICLE: What Is Privacy Worth?, Alessandro Acquisti, Leslie K. John, and George Loewenstein

399. Copyright (c) 2011 Journal of Technology Law & Policy Journal of Technology Law & Policy, June, 2011, Journal of Technology Law & Policy, 16 J. Tech. L. & Pol'y 175, 8284 words, NOTE: OVER-EXPOSED? TSA SCANNERS AND THE FOURTH AMENDMENT RIGHT TO PRIVACY, Jennifer LeVine\*

400. Copyright (c) 2012 Kansas Journal of Law & Public Policy Kansas Journal of Law & Public Policy, Spring, 2012, Kansas Journal of Law & Public Policy, 21 Kan. J.L. & Pub. Pol'y 221, 19420 words, ARTICLE: PROTECTING THE FREEDOM OF INFORMATION ACT REQUESTOR: PRIVACY FOR INFORMATION SEEKERS, Sarah Shik Lamdan\*

401. Copyright (c) 2013 Kansas Law Review, Inc. The University of Kansas Law Review, October, 2013, The University of Kansas Law Review, 62 Kan. L. Rev. 195, 15058 words, COMMENT: United States v. Flores-Lopez: Protecting Privacy Rights in Cell Phone Searches Incident to Arrest\*, Kevin Wempe

402. Copyright (c) 2013 Kansas Law Review, Inc. The University of Kansas Law Review, June, 2013, The University of Kansas Law Review, 61 Kan. L. Rev. 983, 19114 words, ARTICLE: Balancing Employer Business Interests and Employee Privacy Interests: A Survey of Kansas Intrusion on Seclusion Cases in the Employment Context, Pamela V. Keller\*

403. Copyright (c) 2010 Kansas Law Review, Inc. The University of Kansas Law Review, January, 2010, The University of Kansas Law Review, 58 Kan. L. Rev. 415, 30703 words, Article: Private Oppression: How Laws That Protect Privacy Can Lead to Oppression, Teri Dobbins Baxter\*

404. Copyright (c) 2013 University of Kentucky College of Law Kentucky Law Journal, 2013 / 2014, Kentucky Law Journal, 102 Ky. L.J. 161, 12420 words, Note: Watching the Watchmen: Drone Privacy and the Need for Oversight, Ben Jenkins n1

405. Copyright (c) 2010 Board of Trustees of the University of Illinois Law and History Review, November, 2010, Law and History Review, 28 Law & Hist. Rev. 1080, 901 words, BOOK REVIEW: Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy, Norman L. Rosenberg, Macalester College

406. Copyright (c) 2012 American Bar Foundation Law and Social Inquiry, Winter, 2012, Law & Social Inquiry, 37 Law & Soc. Inquiry 119, 15426 words, ARTICLE: Privacy Codes and Institutional Record Keeping: Procedural versus Strategic Approaches, James B. Rule

407. Copyright (c) 2011 American Association of Law Libraries Law Library Journal, Fall, 2011, Law Library Journal, 103 Law Libr. J. 671, 693 words, REVIEW ARTICLE: Keeping Up with New Legal Titles \*: Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists, Compiled by Creighton J. Miller, Jr. \*\* and Annmarie Zell \*\*\* Reviewed by Ellen M. Quinn

408. Copyright (c) 2014 The University of Louisville University of Louisville Law Review, 2014, University of Louisville Law Review, 52 U. Louisville L. Rev. 333, 6602 words, CONSTITUTION SAY REMARKS: PRIVACY AND TECHNOLOGY IN THE TWENTY-FIRST CENTURY, Mark A. Rothstein\*

409. Copyright (c) 2013 Loyola University New Orleans College of Law Loyola Law Review, Spring, 2013, Loyola Law Review, 59 Loy. L. Rev. 157, 20486 words, COMMENT: HOW THE DNA ACT VIOLATES THE FOURTH AMENDMENT RIGHT TO PRIVACY OF MERE ARRESTEES AND PRE-TRIAL DETAINEES, Stephanie Beaugh n222

410. Copyright (c) 2013 Loyola University New Orleans College of Law Loyola Law Review, Winter, 2013, Loyola Law Review, 59 Loy. L. Rev. 861, 38343 words, ARTICLE: NSA SURVEILLANCE SINCE 9/11 AND THE HUMAN RIGHT TO PRIVACY, G. Alex Sinha\*

411. Copyright (c) 2011 Loyola University New Orleans College of Law Loyola Law Review, Spring, 2011, Loyola Law Review, 57 Loy. L. Rev. 1, 14600 words, ARTICLE: THE DANGEROUS TREND BLURRING THE DISTINCTION BETWEEN A REASONABLE EXPECTATION OF CONFIDENTIALITY IN PRIVILEGE LAW AND A REASONABLE EXPECTATION OF PRIVACY IN FOURTH AMENDMENT JURISPRUDENCE, Edward J. Imwinkelried\*

412. Copyright (c) 2010 Loyola of Los Angeles Entertainment Law Review Loyola of Los Angeles Entertainment Law Review, 2010 / 2011, Loyola of Los Angeles Entertainment Law Review, 31 Loy. L.A. Ent. L. Rev. 27, 15029 words, NOTE & COMMENT: UNMASKING THE MASK-MAKER: DOMAIN PRIVACY SERVICES AND CONTRIBUTORY COPYRIGHT INFRINGEMENT, Paulo Andre de Almeida\*

413. Copyright (c) 2013 Loyola Law School Loyola of Los Angeles International & Comparative Law Review, Summer, 2013, Loyola of Los Angeles International & Comparative Law Review, 35 Loy. L.A. Int'l & Comp. L. Rev. 433, 10001 words, ARTICLE: Protecting Speech, Protecting Privacy: The Future Costs of U.K. Libel Claims, ADELAIDE SCARDINO LOPEZ \*

414. Copyright (c) 2011 Loyola Law School Loyola of Los Angeles International & Comparative Law Review, Fall, 2011, Loyola of Los Angeles International & Comparative Law Review, 34 Loy. L.A. Int'l & Comp. L. Rev. 267, 17450 words, NOTE AND COMMENT: The E.U. Model as an Adoptable Approach for U.S. Privacy Laws: A Comparative Analysis of Data Collection Laws in the United Kingdom, Germany, and the United States, LAURA YBARRA \*

415. Copyright (c) 2012 Loyola Law School of Loyola Marymount University Loyola of Los Angeles Law Review, Fall, 2012, Loyola of Los Angeles Law Review, 46 Loy. L.A. L. Rev. 163, 21343 words, ARTICLE: FOUR EASY PIECES TO BALANCE PRIVACY AND ACCOUNTABILITY IN PUBLIC HIGHER EDUCATION: A RESPONSE TO WRONGDOING RANGING FROM PETTY CORRUPTION TO THE SANDUSKY AND PENN STATE TRAGEDY, Robert Steinbuch\*

416. Copyright (c) 2013 Loyola Law School of Loyola Marymount University Loyola of Los Angeles Law Review, Winter, 2013, Loyola of Los Angeles Law Review, 46 Loy. L.A. L. Rev. 739, 7804 words, CASE COMMENT: FAA V. COOPER: HOW THE COURT STRIPPED THE PRIVACY ACT OF ITS PURPOSE AND MEANING, Anna Kim\*

417. Copyright (c) 2012 Loyola Law School of Loyola Marymount University Loyola of Los Angeles Law Review, Winter, 2012, Loyola of Los Angeles Law Review, 45 Loy. L.A. L. Rev. 477, 10441 words, COMMENT: NASA V. NELSON: THE HIGH COURT FLYING HIGH ABOVE THE RIGHT TO INFORMATIONAL PRIVACY, Blythe Golay\*

418. Copyright (c) 2013 Loyola University College of Law Loyola Maritime Law Journal, Winter, 2013, Loyola Maritime Law Journal, 12 Loy. Mar. L.J. 24, 13985 words, ARTICLE: HIPAA, THE PRIVACY RULE AND THEIR IMPLICATIONS UNDER THE LONGSHORE AND HARBOR WORKERS' COMPENSATION ACT, By Robert A. McLaughlin\*

419. Copyright (c) 2014 University of Maine School of Law Maine Law Review, 2014, Maine Law Review, 66 Me. L. Rev. 366, 380 words, SYMPOSIUM: WHO'S GOVERNING PRIVACY? REGULATION AND PROTECTION IN A DIGITAL ERA: INTRODUCTION

420. Copyright (c) 2014 University of Maine School of Law Maine Law Review, 2014, Maine Law Review, 66 Me. L. Rev. 369, 1624 words, SYMPOSIUM: WHO'S GOVERNING PRIVACY? REGULATION AND PROTECTION IN A DIGITAL ERA: FOREWORD, Peter J. Guffin, Esq., Kyle J. Glover, Esq., and Sara M. Benjamin, Esq. \*

421. Copyright (c) 2014 University of Maine School of Law Maine Law Review, 2014, Maine Law Review, 66 Me. L. Rev. 397, 10446 words, ARTICLE: LOCAL LAW ENFORCEMENT JUMPS ON THE BIG DATA BANDWAGON: AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS, INFORMATION PRIVACY, AND ACCESS TO GOVERNMENT INFORMATION, Bryce Clayton Newell \*

422. Copyright (c) 2014 University of Maine School of Law Maine Law Review, 2014, Maine Law Review, 66 Me. L. Rev. 437, 10385 words, ARTICLE: THE PROMISE AND SHORTCOMINGS OF PRIVACY MULTISTAKEHOLDER POLICYMAKING: A CASE STUDY, Omer Tene and J. Trevor Hughes \*

423. Copyright (c) 2014 University of Maine School of Law Maine Law Review, 2014, Maine Law Review, 66 Me. L. Rev. 467, 10559 words, ARTICLE: PRIVACY LAW'S PRECAUTIONARY PRINCIPLE PROBLEM, Adam Thierer \*

424. Copyright (c) 2014 University of Maine School of Law Maine Law Review, 2014, Maine Law Review, 66 Me. L. Rev. 487, 10514 words, ARTICLE: PRIVACY AND SECURITY IN THE CLOUD: SOME REALISM ABOUT TECHNICAL SOLUTIONS TO TRANSNATIONAL SURVEILLANCE IN THE POST-SNOWDEN ERA +, Joris V.J. van Hoboken \* and Ira S. Rubinstein \*\*

425. Copyright (c) 2011 Marquette Law Review Marquette Law Review, Winter, 2011 / 2012, Marquette Law Review, 95 Marq. L. Rev. 751, 19865 words, NOTE: CAR-VING OUT NOTIONS OF PRIVACY: THE IMPACT OF GPS TRACKING AND WHY MAYNARD IS A MOVE IN THE RIGHT DIRECTION, Justin P. Webb\*

426. Copyright (c) 2010 Marquette University Marquette Sports Law Review, Fall, 2010, Marquette Sports Law Review, 21 Marq. Sports L. Rev. 203, 8004 words, SYMPOSIUM: SPORTS LAW: ALUMNI ANALYSIS AND PERSPECTIVES: 140 CHARACTERS OR LESS: MAINTAINING PRIVACY AND PUBLICITY IN THE AGE OF SOCIAL NETWORKING, Lauren McCoy\*

427. Copyright (c) 2013 Maryland Law Review Maryland Law Review, 2013, Maryland Law Review, 72 Md. L. Rev. 335, 21975 words, SPECIAL FEATURE: CYBERLAW: ESSAY: WHY THE RIGHT TO DATA PORTABILITY LIKELY REDUCES CONSUMER WELFARE: ANTITRUST AND PRIVACY CRITIQUE, Peter Swire\* and Yianni Lagos\*\*

428. Copyright (c) 2013 Maryland Law Review Maryland Law Review, 2013, Maryland Law Review, 72 Md. L. Rev. 452, 21495 words, SPECIAL FEATURE: CYBERLAW: ARTICLE: FROM LORD COKE TO INTERNET PRIVACY: THE PAST, PRESENT, AND FUTURE OF THE LAW OF ELECTRONIC CONTRACTING, Juliet M. Moringiello\* and William L. Reynolds\*\*

429. Copyright (c) 2012 Maryland Law Review Maryland Law Review, 2012, Maryland Law Review, 71 Md. L. Rev. 772, 32960 words, ARTICLE: SPECIAL FEATURE: CYBERLAW: SUSTAINING PRIVACY AND OPEN JUSTICE IN THE TRANSITION TO ONLINE COURT RECORDS: A MULTIDISCIPLINARY INQUIRY+, Amanda Conley,\* Anupam Datta,\*\* Helen Nissenbaum\*\*\* and Divya Sharma\*\*\*\*

... arguments. We are also grateful for opportunities to present this work to the NYU **Privacy** Research Group, **Privacy** Law Scholars Conference 2011, and the Conference on **Privacy** and Public Access to Court Records (2008 and 2011). Support ...

430. Copyright (c) 2013 McGill Law Journal Inc. Revue de droit McGill Inc. McGill Law Journal Revue de droit de McGill, September, 2013, McGill Law Journal, 59 McGill L.J. 49, 21967 words, ARTICLE: PRIVACY, CORRECTIVE JUSTICE, AND INCREMENTALISM: LEGAL IMAGINATION AND THE RECOGNITION OF A PRIVACY TORT IN ONTARIO, Thomas DC Bennett\*

431. Copyright (c) 2011 McGill Law Journal Inc. Revue de droit McGill Inc. McGill Law Journal Revue de droit de McGill, February, 2011, McGill Law Journal, 56 McGill L.J. 289, 10379 words, ARTICLE: THE JUDICIAL SYSTEM IN THE DIGITAL AGE: REVISITING THE RELATIONSHIP BETWEEN PRIVACY AND ACCESSIBILITY IN THE CYBER CONTEXT, Karen Eltis\*

432. Copyright (c) 2010 McGill Law Journal Inc. Revue de droit McGill Inc. McGill Law Journal Revue de droit de McGill, July, 2010, McGill Law Journal, 55 McGill L.J. 165, 21947 words, ARTICLE: PRIVACY AND PRIVATE LAW: THE DILEMMA OF JUSTIFICATION, Lisa M. Austin\*

433. Copyright (c) 2013 Walter F. George School of Law, Mercer University Mercer Law Review, Spring, 2013, Mercer Law Review, 64 Mercer L. Rev. 785, 10352 words, Defining and Enforcing the Federal Prosecutor's Duty to Disclose Exculpatory Evidence: Thirteenth Annual Georgia Symposium on Ethics and Professionalism: A Symposium of the Mercer Law Review: Casenote: FAA v. Cooper: Bombarding the Privacy Act with the "Canon of Sovereign Immunity", S. Jacob Carroll

434. Copyright (c) 2011 University of Miami International and Comparative Law Review, Spring, 2011, International & Comparative Law Review\*, 18 U. Miami Int'l & Comp. L. Rev. 137, 16474 words, ARTICLE: [#xBF]VIVA LA DATA PROTECTION? CHILE AS A TOUCHSTONE FOR THE FUTURE OF INFORMATION PRIVACY, Nicola Carah Menaldo

435. Copyright (c) 2012 University of Michigan Law School Michigan Journal of Gender & Law, 2012, Michigan Journal of Gender & Law, 19 Mich. J. Gender & L. 71, 38140 words, Article: The Devil Comes to Kansas: A Story of Free Love, Sexual Privacy, and the Law, Charles J. Reid, Jr.\*

436. Copyright (c) 2011 University of Michigan Journal of Law Reform Online University of Michigan Journal of Law Reform Online, 2011, University of Michigan Journal of Law Reform Online, 1 U. Mich. J.L. Reform 12A, 525 words, COMMENT: THE LATEST 4TH AMENDMENT PRIVACY CONUNDRUM: "STINGRAYS", Max Bulinski \*

437. Copyright (c) 2013 Michigan Law Review Association Michigan Law Review, February, 2013, Michigan Law Review, 111 Mich. L. Rev. 485, 28656 words, ARTICLE: The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions, Erin Murphy\*

438. Copyright (c) 2013 Michigan Law Review Association Michigan Law Review, April, 2013, Michigan Law Review, 111 Mich. L. Rev. 1021, 11043 words, 2013 SURVEY OF BOOKS RELATED TO THE LAW: BOOK REVIEW: THE FIGHT TO FRAME PRIVACY, Woodrow Hartzog\*

Nothing to Hide: The False Tradeoff Between **Privacy** and Security. By Daniel J. Solove. New Haven and ...

439. Copyright (c) 2011 Michigan Law Review Association Michigan Law Review, April, 2011, Michigan Law Review, 109 Mich. L. Rev. 979, 6484 words, 2011 SURVEY OF BOOKS RELATED TO THE LAW: REVIEW: SUK: AT HOME IN THE LAW: HOW THE DOMESTIC VIOLENCE REVOLUTION IS TRANSFORMING PRIVACY, + Copyright © 2010 by I. Bennett Capers., I. Bennett Capers\*

... in the Law: How the Domestic Violence Revolution Is Transforming **Privacy.** By Jeannie Suk. New Haven and London: Yale ...

440. Copyright (c) 2010 Michigan Law Review Association Michigan Law Review, April, 2010, Michigan Law Review, 108 Mich. L. Rev. 1107, 9643 words, REVIEW: VISIONARY PRAGMATISM AND THE VALUE OF PRIVACY IN THE TWENTY-FIRST CENTURY, Danielle Keats Citron\* and Leslie Meltzer Henry\*\*

441. Copyright (c) 2013 Michigan State University College of Law Michigan State Law Review, 2013, Michigan State Law Review, 2013 Mich. St. L. Rev. 83, 43979 words, ARTICLE: GOING DUTCH? COLLABORATIVE DUTCH PRIVACY REGULATION AND THE LESSONS IT HOLDS FOR U.S. PRIVACY LAW, Dennis D. Hirsch\*

442. Copyright (c) 2010 Michigan State University College of Law Michigan State Law Review, Summer, 2010, Michigan State Law Review, 2010 Mich. St. L. Rev. 311, 16377 words, ARTICLE: SALVAGING PRIVACY & TRANQUILITY FROM THE WRECKAGE: IMAGES OF DEATH, EMOTIONS OF DISTRESS & REMEDIES OF TORT IN THE AGE OF THE INTERNET, Clay Calvert\*

443. Copyright (c) 2012 Midwest Academy of Legal Studies in Business. All Rights Reserved. Midwest Law Journal, Spring, 2012, Midwest Law Journal, 26 Midwest L.J. 27, 16340 words, ARTICLE: PRIVACY FOR WORKPLACE COMMUNICATION IN A DIGITAL AGE: CAN THERE BE HUMAN DIGNITY WHILE DRESSED IN THE EMPEROR'S NEW CLOTHES?, CAROL M. BAST n1 AND CYNTHIA A. BROWN n2

444. Copyright (c) 2012 University of Michigan Law School Michigan Telecommunications and Technology Law Review, Fall, 2012, Michigan Telecommunications & Technology Law Review, 19 Mich. Telecomm. Tech. L. Rev. 163, 19430 words, NOTE: PRIVACY POLICIES, TERMS OF SERVICE, AND FTC ENFORCEMENT: BROADENING UNFAIRNESS REGULATION FOR A NEW ERA, G.S. Hans\*

445. Copyright (c) 2011 University of Michigan Law School Michigan Telecommunications and Technology Law Review, Spring, 2011, Michigan Telecommunications & Technology Law Review, 17 Mich. Telecomm. Tech. L. Rev. 337, 21423 words, ARTICLE: DOES LAW MATTER ONLINE? EMPIRICAL EVIDENCE ON PRIVACY LAW COMPLIANCE, Michael Birnhack\* and Niva Elkin-Koren\*\*

446. Copyright (c) 2010 University of Michigan Law School Michigan Telecommunications and Technology Law Review, Spring, 2010, Michigan Telecommunications and Technology Law Review, 16 Mich. Telecomm. Tech. L. Rev. 279, 36005 words, ARTICLE: THERE IS A TIME TO KEEP SILENT AND A TIME TO SPEAK, THE HARD PART IS KNOWING WHICH IS WHICH: STRIKING THE BALANCE BETWEEN PRIVACY PROTECTION AND THE FLOW OF HEALTH CARE INFORMATION, Daniel J. Gilman\* James C. Cooper\*\*

447. Copyright (c) 2014 Minnesota Journal of Law, Science & Technology Minnesota Journal of Law, Science & Technology, Spring, 2014, Minnesota Journal of Law, Science & Technology, 15 Minn. J.L. Sci. & Tech. 949, 10485 words, ARTICLE: The Times They Are a-Changin': Shifting Norms and Employee Privacy in the Technological Era, Lisa M. Durham Taylor \*

448. Copyright (c) 2014 Minnesota Journal of Law, Science & Technology Minnesota Journal of Law, Science & Technology, Spring, 2014, Minnesota Journal of Law, Science & Technology, 15 Minn. J.L. Sci. & Tech. 1155, 10432 words, COMMENT: Aligning Online Privacy Protection with Reasonable Expectations of Privacy: How Joffe Can Be Used to Modernize the Wiretap Act, Matthew Mason \*

449. Copyright (c) 2012 Minnesota Journal of Law, Science & Technology Minnesota Journal of Law, Science & Technology, Spring, 2012, Minnesota Journal of Law, Science & Technology, 13 Minn. J.L. Sci. & Tech. 867, 13986 words, NOTE & COMMENT: It's the Autonomy, Stupid: Political Data-Mining and Voter Privacy in the Information Age, Chris Evans\*

450. Copyright (c) 2011 Minnesota Journal of Law, Science & Technology Minnesota Journal of Law, Science & Technology, Winter, 2011, Minnesota Journal of Law, Science and Technology, 12 Minn. J.L. Sci. & Tech. 191, 18102 words, Article: An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government, Christopher Soghoian\*

451. Copyright (c) 2013 Minnesota Law Review Foundation Minnesota Law Review, November, 2013, Minnesota Law Review, 98 Minn. L. Rev. 62, 35919 words, Article: The Right to Quantitative Privacy, David Gray+ and Danielle Citron++

452. Copyright (c) 2014 Minnesota Law Review Foundation Minnesota Law Review, June, 2014, Minnesota Law Review, 98 Minn. L. Rev. 2375, 16452 words, Note: HIPAA-Cratic or HIPAA-Critical: U.S. Privacy Protections Should Be Guaranteed By Covered Entities Working Abroad, Grace Fleming\*

453. Copyright (c) 2013 Minnesota Law Review Foundation Minnesota Law Review, February, 2013, Minnesota Law Review, 97 Minn. L. Rev. 907, 38713 words, Article: Branding Privacy, Paul Ohm+

454. Copyright (c) 2010 Minnesota Law Review Foundation Minnesota Law Review, December, 2010, Minnesota Law Review, 95 Minn. L. Rev. 682, 14266 words, Article: Relative Futility: Limits to Genetic Privacy Protection Because of the Inability to Prevent Disclosure of Genetic Information by Relatives, Trevor Woodage\*

455. Copyright (c) 2010 Minnesota Law Review Foundation Minnesota Law Review, May, 2010, Minnesota Law Review, 94 Minn. L. Rev. 1303, 1856 words, SYMPOSIUM CYBERSPACE & THE LAW: PRIVACY, PROPERTY, AND CRIME IN THE VIRTUAL FRONTIER: Foreword, Nicole M. Murphy\*

456. Copyright (c) 2010 Minnesota Law Review Foundation Minnesota Law Review, May, 2010, Minnesota Law Review, 94 Minn. L. Rev. 1308, 26169 words, SYMPOSIUM CYBERSPACE & THE LAW: PRIVACY, PROPERTY, AND CRIME IN THE VIRTUAL FRONTIER: Google Book Search and the Future of Books in Cyberspace, Pamela Samuelson +

457. Copyright (c) 2010 Minnesota Law Review Foundation Minnesota Law Review, May, 2010, Minnesota Law Review, 94 Minn. L. Rev. 1375, 21677 words, SYMPOSIUM CYBERSPACE & THE LAW: PRIVACY, PROPERTY, AND CRIME IN THE VIRTUAL FRONTIER: Cybermarks, Dan L. Burk +

458. Copyright (c) 2010 Minnesota Law Review Foundation Minnesota Law Review, May, 2010, Minnesota Law Review, 94 Minn. L. Rev. 1417, 26151 words, SYMPOSIUM CYBERSPACE & THE LAW: PRIVACY, PROPERTY, AND CRIME IN THE VIRTUAL FRONTIER: The Implications for Law of User Innovation, William W. Fisher III +

459. Copyright (c) 2010 Minnesota Law Review Foundation Minnesota Law Review, May, 2010, Minnesota Law Review, 94 Minn. L. Rev. 1478, 18003 words, SYMPOSIUM CYBERSPACE & THE LAW: PRIVACY, PROPERTY, AND CRIME IN THE VIRTUAL FRONTIER: Mask, Shield, and Sword: Should the Journalist's Privilege Protect the Identity of Anonymous Posters to News Media Websites?, Jane E. Kirtley +

460. Copyright (c) 2010 Minnesota Law Review Foundation Minnesota Law Review, May, 2010, Minnesota Law Review, 94 Minn. L. Rev. 1514, 21139 words, SYMPOSIUM CYBERSPACE & THE LAW: PRIVACY, PROPERTY, AND CRIME IN THE VIRTUAL FRONTIER: Probably Probable Cause: The Diminishing Importance of Justification Standards, Paul Ohm +

461. Copyright (c) 2010 Minnesota Law Review Foundation Minnesota Law Review, May, 2010, Minnesota Law Review, 94 Minn. L. Rev. 1561, 14178 words, SYMPOSIUM CYBERSPACE & THE LAW: PRIVACY, PROPERTY, AND CRIME IN THE VIRTUAL FRONTIER: Vagueness Challenges to the Computer Fraud and Abuse Act, Orin S. Kerr +

462. Copyright (c) 2010 Minnesota Law Review Foundation Minnesota Law Review, May, 2010, Minnesota Law Review, 94 Minn. L. Rev. 1588, 14483 words, SYMPOSIUM CYBERSPACE & THE LAW: PRIVACY, PROPERTY, AND CRIME IN THE VIRTUAL FRONTIER: Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire, Christopher Slobogin +

463. Copyright (c) 2014 Mississippi College Law Review Mississippi College Law Review, 2014, Mississippi College Law Review, 32 Miss. C. L. Rev. 447, 10566 words, ARTICLE: The Evolution of the Right to Exclude - More than a Property Right, a Privacy Right, Jace C. Gatewood\*

464. Copyright (c) 2012 Mississippi College Law Review Mississippi College Law Review, 2012, Mississippi College Law Review, 31 Miss. C. L. Rev. 227, 11027 words, ARTICLE: Expectations of Privacy in Social Media, Stephen E. Henderson\*

465. Copyright (c) 2013 Mississippi Law Journal, Inc. Mississippi Law Journal, 2013, Mississippi Law Journal, 82 Miss. L.J. 975, 11190 words, ARTICLE: PRIVACY IN AN AGE OF ADVANCING TECHNOLOGY, Russell L. Weaver \*

466. Copyright (c) 2012 Mississippi Law Journal, Inc. Mississippi Law Journal, Symposium, 2012, Mississippi Law Journal, 81 Miss. L.J. 895, 6694 words, ARTICLE: The Future of Seizure Analysis: BIG BROTHER OR LITTLE BROTHER? SURRENDERING SEIZURE PRIVACY FOR THE BENEFITS OF COMMUNICATION TECHNOLOGY, Jose Felipe Anderson\*

467. Copyright (c) 2012 Mississippi Law Journal, Inc. Mississippi Law Journal, Symposium, 2012, Mississippi Law Journal, 81 Miss. L.J. 971, 7705 words, ARTICLE: The Future of Search Analysis: WESTERN UNION, THE AMERICAN FEDERATION OF LABOR, GOOGLE, AND THE CHANGING FACE OF PRIVACY ADVOCATES, Wesley MacNeil Oliver\*

468. Copyright (c) 2012 Mississippi Law Journal, Inc. Mississippi Law Journal, Symposium, 2012, Mississippi Law Journal, 81 Miss. L.J. 1309, 19265 words, ARTICLE: The Future of Digital Evidence Searches and Seizures: THE FOURTH AMENDMENT IN A WORLD WITHOUT PRIVACY, Paul Ohm\*

469. Copyright (c) 2012 Mississippi Law Journal, Inc. Mississippi Law Journal, Symposium, 2012, Mississippi Law Journal, 81 Miss. L.J. 1359, 28376 words, ARTICLE: THE JAMES OTIS LECTURE: ELECTRONIC PRIVACY IN THE GOVERNMENT WORKPLACE AND CITY OF ONTARIO, CALIFORNIA V. QUON: THE SUPREME COURT BROUGHT FORTH A MOUSE, Clifford S. Fishman\*

470. Copyright (c) 2010 Mississippi Law Journal, Inc. Mississippi Law Journal, Fall, 2010, Mississippi Law Journal, 80 Miss. L.J. 299, 17817 words, ARTICLE: HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12, BACKGROUND INVESTIGATIONS, AND INFORMATIONAL PRIVACY RIGHTS, Colin M. O'Brien \*

471. Copyright (c) 2011 Mississippi Law Journal, Inc. Mississippi Law Journal, Spring, 2011, Mississippi Law Journal, 80 Miss. L.J. 1033, 22813 words, ARTICLE: REASONABLE EXPECTATIONS OF PRIVACY FOR YOUTH IN A DIGITAL AGE, Mary Graw Leary \*

472. Copyright (c) 2011 Mississippi Law Journal, Inc. Mississippi Law Journal, Spring, 2011, Mississippi Law Journal, 80 Miss. L.J. 1129, 41543 words, ARTICLE: THE FOURTH AMENDMENT, PRIVACY AND ADVANCING TECHNOLOGY, Russell L. Weaver \*

473. Copyright (c) 2012 Curators of the University of Missouri UMKC Law Review, Winter, 2012, UMKC Law Review, 81 UMKC L. Rev. 385, 16386 words, SYMPOSIUM: THE NEXT FOUR YEARS: A CROSS-PRACTICE ANALYSIS OF LEGAL ISSUES RELEVANT TO THIS PRESIDENTIAL TERM: ARTICLE: PROTECTING PATIENT PRIVACY IN THE AGE OF BIG DATA, Nicolas P. Terry\*

474. Copyright (c) 2014 The University of Montana School of Law Montana Law Review, Summer, 2014, Montana Law Review, 75 Mont. L. Rev. 297, 10674 words, ESSAY: THE SHAME GAME: MONTANA'S RIGHT TO PRIVACY FOR LEVEL 1 SEX OFFENDERS, Johnna Preble\*

475. Copyright (c) 2012 The University of Montana School of Law Montana Law Review, Winter, 2012, Montana Law Review, 73 Mont. L. Rev. 179, 12010 words, NOTE: STATE v. ALLEN: THE CONNECTION BETWEEN THE RIGHT TO BE SECURE FROM UNREASONABLE SEARCHES AND SEIZURES AND MONTANA'S INDIVIDUAL RIGHT OF PRIVACY, Stephanie Holstein\*

476. Copyright (c) 2010 Naval Law Review, 2010, Naval Law Review, 60 Naval L. Rev. 93, 19353 words, ARTICLE, ESSAY & NOTE: THE SHIPBOARD PANDORA'S BOX: THE OPERATIONAL REALITY THAT AN EXPECTATION OF PRIVACY EXISTS IN ELECTRONIC COMMUNICATIONS ABOARD NAVAL VESSELS, Lieutenant Colonel Leon James Francis n1

477. Copyright (c) 2014 University of Nebraska Nebraska Law Review, 2014, Nebraska Law Review, 92 Neb. L. Rev. 504, 16746 words, ARTICLE: District of Columbia Jones and the Mosaic Theory - In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory, Jace C. Gatewood\*[bns

478. Copyright (c) 2014 University of Nebraska Nebraska Law Review, 2014, Nebraska Law Review, 92 Neb. L. Rev. 746, 26122 words, ARTICLE: Intellectual Property's Lessons for Information Privacy, Mark Bartholomew\*

479. Copyright (c) 2011 University of Nebraska Nebraska Law Review, 2011, Nebraska Law Review, 90 Neb. L. Rev. 559, 15576 words, Note\*: Did My Boss Just Read That? Applying a Coding vs. Content Distinction in Determining Government Employees' Reasonable Expectation of Privacy in Employer-Provided Electronic Communication Devices After City of Ontario v. Quon, 130 S. Ct. 2619 (2010), Lori Hoetger

480. Copyright (c) 2014 New England School of Law New England Journal on Criminal and Civil Confinement, Winter, 2014, New England Journal on Criminal & Civil Confinement, 40 N.E. J. on Crim. & Civ. Con. 135, 15042 words, Note: The Place Where There is No Darkness: Privacy and Protest in the Age of Social Media, William Carius\*

481. Copyright (c) 2013 New England School of Law New England Law Review, Spring, 2013, New England Law Review, 47 New Eng. L. Rev. 773, 11151 words, COMMENT: While You Were Out: You Were Evicted - The Demise of Hotel Privacy in Commonwealth v. Molina, Alaina Anderson\*

482. Copyright (c) 2010 New England School of Law New England Law Review, Summer, 2010, New England Law Review, 44 New Eng. L. Rev. 971, 11759 words, COMMENT: ALL THE VICE PRESIDENT'S MEN: HOW THE COURT IN WILSON V. LIBBY MISINTERPRETED THE PRIVACY ACT AND DENIED A REMEDY FOR THE ILLEGAL DISCLOSURE OF VALERIE PLAME WILSON'S COVERT CIA IDENTITY, Kristin I. Oickle\*

483. Copyright (c) 2011 The New Hampshire Bar Association New Hampshire Bar Journal, Summer, 2011, 52 N.H.B.J. 28, 10567 words, ARTICLE: PRIVACY AND DATA SECURITY: NEW CHALLENGES OF THE DIGITAL AGE, By Cameron G. Shilling n1

484. Copyright (c) 2010 New York University Annual Survey of American Law New York University Annual Survey of American Law, 2010, New York University Annual Survey of American Law, 66 N.Y.U. Ann. Surv. Am. L. 173, 19788 words, NOTE: TWILIGHT: THE FADING OF FALSE LIGHT INVASION OF PRIVACY, ANDREW OSORIO\*

485. Copyright 2010 New York University Journal of Law & Liberty NYU Journal of Law & Liberty, 2010, NYU Journal of Law & Liberty, 5 NYU J.L. & Liberty 638, 15791 words, ARTICLE: Pragmatism and Privacy, Amy L. Peikoff\*

486. Copyright (c) 2012 New York University Law Review New York University Law Review, December, 2012, New York University Law Review, 87 N.Y.U.L. Rev. 1918, 14038 words, NOTE: ENTRENCHING PRIVACY: A CRITIQUE OF CIVIL REMEDIES FOR GENDER-MOTIVATED VIOLENCE, Lauren M. Gambier\*

487. Copyright (c) 2011 New York University Law Review New York University Law Review, December, 2011, New York University Law Review, 86 N.Y.U.L. Rev. 1814, 40176 words, ARTICLE: THE PII PROBLEM: PRIVACY AND A NEW CONCEPT OF PERSONALLY IDENTIFIABLE INFORMATION, Paul M. Schwartz+ & Daniel J. Solove++

488. Copyright (c) 2012 New York University Review of Law & Social Change New York University Review of Law & Social Change, 2012, New York University Review of Law & Social Change, 36 N.Y.U. Rev. L. & Soc. Change 215, 34873 words, ARTICLE: PUTTING ONLINE PRIVACY ABOVE THE FOLD: BUILDING A SOCIAL MOVEMENT AND CREATING CORPORATE CHANGE, Nicole A. Ozer+

489. Copyright (c) 2011 Legal Research Foundation Inc. New Zealand Law Review, 2011, New Zealand Law Review, 2011 NZ Law Review 69, 10284 words, ARTICLE: Criminal Records, Spent Convictions and Privacy: A Trans-Tasman Comparison, MOIRA PATERSON \*

490. Copyright (c) 2012 Chapman University School of Law Nexus: Chapman's Journal of Law & Policy, 2012 / 2013, Nexus: Chapman's Journal of Law & Policy, 18 Nexus J. Op. 81, 19200 words, Healthy Decision or Unhealthy Oversight?: A Legal Debate on the Patient Protection and Affordable Care Act and the Impact of the Supreme Court's Recent Decision: The Diminished Privacy Rights of Welfare Recipients: Legitimacy Derived From Sources Beyond Legality, By Stephanie Brault\*

491. Copyright (c) 2013 North Carolina Journal of Law & Technology North Carolina Journal of Law & Technology, Spring, 2013, North Carolina Journal of Law & Technology, 14 N.C. J.L. & Tech. 381, 18974 words, ARTICLE: A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy, David Gray\* and Danielle Keats Citron\*\*

492. Copyright (c) 2013 North Carolina Journal of Law & Technology North Carolina Journal of Law & Technology, Spring, 2013, North Carolina Journal of Law & Technology, 14 N.C. J.L. & Tech. 489, 26556 words, ARTICLE: Jonesing for a Privacy Mandate, Getting a Technology Fix - Doctrine to Follow, Stephanie K. Pell\*

493. Copyright (c) 2010 North Carolina Journal of Law & Technology North Carolina Journal of Law & Technology, 2010, North Carolina Journal of Law & Technology, 11 N.C. J.L. & Tech. 553, 3605 words, ARTICLE: Library Standards for Privacy: A Model for the Digital World?, Anne Klinefelter\*

494. Copyright (c) 2012 North Carolina Law Review Association North Carolina Law Review, June, 2012, North Carolina Law Review, 90 N.C.L. Rev. 1295, 5161 words, CONTENT: SOCIAL NETWORKS AND THE LAW: KEYNOTE: PRIVACY & CONSUMER PROTECTION IN SOCIAL MEDIA\*, Julie Brill\*\*

495. Copyright (c) 2012 North Carolina Law Review Association North Carolina Law Review, June, 2012, North Carolina Law Review, 90 N.C.L. Rev. 1309, 6900 words, CONTENT: SOCIAL NETWORKS AND THE LAW: REMARKS: Putting Consumers at the Heart of the Social Media Revolution: Toward A Personal Property Interest to Protect Privacy\*, Remarks by Timothy D. Sparapani\*\*

496. Copyright (c) 2012 North Carolina Law Review Association North Carolina Law Review, June, 2012, North Carolina Law Review, 90 N.C.L. Rev. 1327, 17482 words, CONTENT: SOCIAL NETWORKS AND THE LAW: UNPACKING PRIVACY'S PRICE\*, Jan Whittington\*\* and Chris Jay Hoofnagle\*\*\*

497. Copyright (c) 2012 North Carolina Law Review Association North Carolina Law Review, June, 2012, North Carolina Law Review, 90 N.C.L. Rev. 1371, 18787 words, CONTENT: SOCIAL NETWORKS AND THE LAW: SOCIAL NETWORKS, PRIVACY, AND FREEDOM OF ASSOCIATION: DATA PROTECTION VS. DATA EMPOWERMENT\*, Peter Swire\*\*

498. Copyright (c) 2012 North Carolina Law Review Association North Carolina Law Review, June, 2012, North Carolina Law Review, 90 N.C.L. Rev. 1417, 15101 words, CONTENT: SOCIAL NETWORKS AND THE LAW: DIFFERENTIAL PRIVACY AS A RESPONSE TO THE REIDENTIFICATION THREAT: THE FACEBOOK ADVERTISER CASE STUDY\*, Andrew Chin\*\* and Anne Klinefelter\*\*\*

499. Copyright (c) 2013 Northern Kentucky University Northern Kentucky Law Review, 2013, Northern Kentucky Law Review, 40 N. Ky. L. Rev. 507, 9466 words, LAW + INFORMATICS SYMPOSIUM ON LABOR AND EMPLOYMENT ISSUES: ARTICLE: A Call for Uncle Sam to Get Big Brother Out of Our Knickers: Protecting Privacy and Freedom of Speech Interests in Social Media Accounts, Michelle Poore\*

500. Copyright (c) 2013 Northern Kentucky University Northern Kentucky Law Review, 2013, Northern Kentucky Law Review, 40 N. Ky. L. Rev. 593, 15195 words, LAW + INFORMATICS SYMPOSIUM ON LABOR AND EMPLOYMENT ISSUES: ARTICLE: Employer Surveillance Versus Employee Privacy: The New Reality of Social Media and Workplace Privacy, Saby Ghoshray\*

501. Copyright (c) 2013 Northern Kentucky University Northern Kentucky Law Review, 2013, Northern Kentucky Law Review, 40 N. Ky. L. Rev. 635, 17720 words, LAW + INFORMATICS SYMPOSIUM ON LABOR AND EMPLOYMENT ISSUES: NOTE: Protecting Privacy of Medical Records of Employees and Job Applicants in the Digital Era Under the Americans With Disabilities Act, Michael L. Tudor\*

502. Copyright (c) 2012 Northern Kentucky University Northern Kentucky Law Review, 2012, Northern Kentucky Law Review, 39 N. Ky. L. Rev. 189, 13921 words, 2012 LAW & INFORMATICS ISSUE: ARTICLE: Privacy and Confidentiality Issues in Historical Health Sciences Collections, Anne T. Gilliland\* and Judith A. Wiener\*\*

503. Copyright (c) 2010 Northern Kentucky University Northern Kentucky Law Review, 2010, Northern Kentucky Law Review, 37 N. Ky. L. Rev. 287, 22927 words, Kentucky Survey Issue: Article: Off-Duty Privacy: How Far Can Employers Go?, Kelly Schoening\* and Kelli Kleisinger\*\*

504. Copyright (c) 2010 Northwestern University School of Law Northwestern Journal of Law and Social Policy, Fall, 2010, Northwestern Journal of Law and Social Policy, 5 Nw. J. L. & Soc. Pol'y 369, 22897 words, Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era, Lauren A. Matecki \*

505. Copyright (c) 2013 Board of Trustees, for Northern Illinois University Northern Illinois University Law Review, Spring, 2013, Northern Illinois University Law Review, 33 N. Ill. U. L. Rev. 563, 6090 words, ARTICLE: New Private Privacy Intrusions in Illinois During Prelitigation Civil Claim Investigations, JEFFREY A. PARNESS n1

506. Copyright (c) 2010 Board of Trustees, for Northern Illinois University Northern Illinois University Law Review, Summer, 2010, Northern Illinois University Law Review, 30 N. Ill. U. L. Rev. 531, 10978 words, SYMPOSIUM: WHAT IT MEANS TO BE A LAWYER IN THE DIGITAL AGE: Article: How the Lack of Prescriptive Technical Granularity in HIPAA Has Compromised Patient Privacy, Tim Wafa\*

507. Copyright (c) 2013 Northwestern University School of Law Northwestern University Law Review, Fall, 2013, Northwestern University Law Review, 108 Nw. U.L. Rev. 343, 19138 words, Note and Comment: MUG SHOT DISCLOSURE UNDER FOIA: DOES PRIVACY OR PUBLIC INTEREST PREVAIL?, Kathryn Shephard

508. Copyright (c) 2013 Northwestern University School of Law Northwestern University Law Review, Spring, 2013, Northwestern University Law Review, 107 Nw. U.L. Rev. 1437, 15935 words, Note and Comment: REVIVING THE PRIVACY PROTECTION ACT OF 1980, Elizabeth B. Uzelac

509. Copyright (c) 2011 Northwestern University School of Law Northwestern University Law Review, Summer, 2011, Northwestern University Law Review, 105 Nw. U.L. Rev. 1153, 25687 words, ARTICLE: UNRAVELING PRIVACY: THE PERSONAL PROSPECTUS AND THE THREAT OF A FULL-DISCLOSURE FUTURE, Scott R. Peppet\*

510. Copyright (c) 2010 Northwestern University School of Law Northwestern University Law Review, Spring, 2010, Northwestern University Law Review, 104 Nw. U.L. Rev. 477, 20295 words, SYMPOSIUM: MAPPING ONLINE PRIVACY, Jacqueline D. Lipton\*

511. Copyright (c) 2010 Northwestern University Law Review Northwestern University Law Review Colloquy, August, 2010, Northwestern University Law Review Colloquy, 105 Nw. U. L. Rev. Colloquy 18, 6569 words, ARTICLE: DYING FOR PRIVACY: PITTING PUBLIC ACCESS AGAINST FAMILIAL INTERESTS IN THE ERA OF THE INTERNET, Clay Calvert \*

512. Copyright (c) 2012 Notre Dame Law Review Notre Dame Law Review, November, 2012, Notre Dame Law Review, 88 Notre Dame L. Rev. 277, 18997 words, ARTICLE: PRIVATIZING WORKPLACE PRIVACY, Paul M. Secunda\*

513. Copyright (c) 2012 Notre Dame Law Review Notre Dame Law Review, February, 2012, Notre Dame Law Review, 87 Notre Dame L. Rev. 1027, 21771 words, ARTICLE: AGAINST NOTICE SKEPTICISM IN PRIVACY (AND ELSEWHERE), M. Ryan Calo\*

514. Copyright (c) 2011 Notre Dame Law Review Notre Dame Law Review, September, 2011, Notre Dame Law Review, 86 Notre Dame L. Rev. 2189, 14038 words, NOTE: CLOUD COVER: PRIVACY PROTECTIONS AND THE STORED COMMUNICATIONS ACT IN THE AGE OF CLOUD COMPUTING, Hien Timothy M. Nguyen\*

515. Copyright (c) 2012 Nova Law Review Nova Law Review, Summer, 2012, Nova Law Review, 36 Nova L. Rev. 521, 20111 words, ARTICLE: A Look at the Proposed Electronic Communications Privacy Act Amendments Act of 2011: Where is Smart Grid Technology, and How Does Inevitable Discovery Apply?, Darlene Bedley\*

516. Copyright (c) 2012 Ohio State Journal on Dispute Resolution Ohio State Journal on Dispute Resolution, 2012, Ohio State Journal on Dispute Resolution, 27 Ohio St. J. on Disp. Resol. 539, 39038 words, ARTICLE: Confidentiality in Mediation: An Application of the Right to Privacy, Susan Oberman\*

517. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 669, 15966 words, Note: Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy, Jonathan Olivito\*

518. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 841, 5893 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Symposium Introduction, Peter Swire\*

519. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 853, 20118 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People's Republic of China, Ann Bartow\*

520. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 897, 10694 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: In the Beginning . . . An Early History of the Privacy Profession, Andrew Clearwater & J. Trevor Hughes\*

521. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 923, 22136 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Hero or Villain: The Data Controller in Privacy Law and Technologies, Claudia Diaz,\* Omer Tene+ & Seda Gurses++ n997

522. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 965, 14327 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology, A. Michael Froomkin\*

523. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 995, 14239 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Social Data, Woodrow Hartzog\*

524. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 1029, 22255 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector- Based Codes of Conduct, Dennis D. Hirsch\*

525. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 1071, 17146 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques, Gus Hosein\* & Caroline Wilson Palow+

526. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 1105, 27386 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Immigration Policing and Federalism Through the Lens of Technology, Surveillance, and Privacy, Anil Kalhan\*

527. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 1167, 12541 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard, Bartosz M. Marcinkowski\*

528. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 1195, 10821 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Deep Pockets, Packets, and Harbors, Thomas Margoni & Mark Perry\*

529. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 1217, 22530 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws, Omer Tene\*

530. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 1263, 22187 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Naked in Front of the Machine: Does Airport Scanning Violate Privacy?, Yofi Tirosh\* and Michael Birnhack+

531. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 1307, 13208 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: From Facebook Regrets to Facebook Privacy Nudges, Yang Wang, Pedro Giovanni Leon, Xiaoxuan Chen, Saranga Komanduri, Gregory Norcie, Kevin Scott, Alessandro Acquisti, Lorrie Faith Cranor & Norman Sadeh\*

532. Copyright (c) 2013 The Ohio State University Ohio State Law Journal, 2013, Ohio State Law Journal, 74 Ohio St. L.J. 1335, 35130 words, SYMPOSIUM: The Second Wave of Global Privacy Protection: Regulating Electronic Identity Intermediaries: The "Soft eID" Conundrum, Tal Z. Zarsky\* and Norberto Nuno Gomes de Andrade+

533. Copyright (c) 2012 Oklahoma City University Oklahoma City University Law Review, Fall, 2012, Oklahoma City University Law Review, 37 Okla. City U.L. Rev. 513, 17083 words, NOTE: Rocking the Cradle with the Right to Privacy: Ensuring Family Protection from Third-Party Surveillance, Sarah E. Hance\*

534. Copyright (c) 2011 Oklahoma City University Oklahoma City University Law Review, Summer, 2011, Oklahoma City University Law Review, 36 Okla. City U.L. Rev. 395, 11436 words, ARTICLE: A Virtual Property Solution: How Privacy Law Can Protect the Citizens of Virtual Worlds, John William Nelson\*

535. Copyright (c) 2013 Oklahoma Law Review Oklahoma Law Review, Winter, 2013, Oklahoma Law Review, 65 Okla. L. Rev. 177, 23464 words, ARTICLE: THE NEXT BATTLEGROUND? PERSONHOOD, PRIVACY, AND ASSISTED REPRODUCTIVE TECHNOLOGIES, Mark Strasser\*

536. Copyright (c) 2012 University of Oregon Oregon Law Review, 2012, Oregon Law Review, 90 Or. L. Rev. 1135, 5055 words, ARTICLE: The (Continued) Assault on Privacy: A Timely Book Review Forty Years in the Making, ALEX KOZINSKI\* and STEPHANIE GRACE+

537. Copyright (c) 2011 Pace University School of Law Pace International Law Review, Winter, 2011, Pace International Law Review, 23 Pace Int'l L. Rev. 215, 17008 words, COMMENT: INTERSEXUALITY AND GENDER VERIFICATION TESTS: THE NEED TO ASSURE HUMAN RIGHTS AND PRIVACY, Stacy Larson

538. Copyright (c) 2013 Pace University School of Law Pace Law Review, Summer, 2013, Pace Law Review, 33 Pace L. Rev. 1146, 9995 words, ARTICLE: The Expanded Use of Wiretap Evidence in White-Collar Prosecutions: Rebalancing Privacy Through More Vigorous Enforcement of the Predicate Offense Requirement and the Suppression Provisions of Title III, Kyle G. Grimm, Esq. \*

539. Copyright (c) 2011 Pace University School of Law Pace Law Review, Winter, 2011, Pace Law Review, 31 Pace L. Rev. 146, 14811 words, SOCIAL NETWORKING AND THE LAW: ARTICLE: "You already have zero privacy. Get over it!" n1 Would Warren and Brandeis Argue for Privacy for Social Networking?, Connie Davis Powell\*

540. Copyright (c) 2011 Pace University School of Law Pace Law Review, Winter, 2011, Pace Law Review, 31 Pace L. Rev. 291, 33283 words, SOCIAL NETWORKING AND THE LAW: ARTICLE: From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance, Junichi P. Semitsu\*

541. Copyright (c) 2010 Pace University School of Law Pace Law Review, Spring, 2010, Pace Law Review, 30 Pace L. Rev. 927, 18346 words, ARTICLE: Privacy Revisited: GPS Tracking as Search and Seizure, Bennett L. Gershman\*

542. Copyright (c) 2011 University of the Pacific, McGeorge School of Law Pacific McGeorge Global Business & Development Law Journal, 2011, Pacific McGeorge Global Business & Development Law Journal, 24 Pac. McGeorge Global Bus. & Dev. L.J. 411, 22673 words, COMMENT: BlackBerry's Jam: Research In Motion's Struggle to Protect Smartphone Users' Internet Privacy Highlights Need for Shared Industry Standards, Darren R. Sweetwood\*

543. Copyright (c) 2014 University of Pennsylvania Journal of Constitutional Law University of Pennsylvania Journal of Constitutional Law, February, 2014, University of Pennsylvania Journal of Constitutional Law, 16 U. Pa. J. Const. L. 805, 14655 words, COMMENT: Informational Privacy: Lessons from Across the Atlantic, Timothy Azarchs\*

544. Copyright (c) 2012 University of Pennsylvania Journal of Constitutional Law University of Pennsylvania Journal of Constitutional Law, February, 2012, University of Pennsylvania Journal of Constitutional Law, 14 U. Pa. J. Const. L. 849, 14757 words, COMMENT: A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use, Alexander Naito\*

545. Copyright (c) 2012 University of Pennsylvania Journal of Constitutional Law University of Pennsylvania Journal of Constitutional Law, March, 2012, University of Pennsylvania Journal of Constitutional Law, 14 U. Pa. J. Const. L. 885, 18170 words, SYMPOSIUM: PRIVACY JURISPRUDENCE AS AN INSTRUMENT OF SOCIAL CHANGE: First Amendment Privacy and the Battle for Progressively Liberal Social Change, Anita L. Allen\*

546. Copyright (c) 2012 University of Pennsylvania Journal of Constitutional Law University of Pennsylvania Journal of Constitutional Law, March, 2012, University of Pennsylvania Journal of Constitutional Law, 14 U. Pa. J. Const. L. 929, 11171 words, SYMPOSIUM: PRIVACY JURISPRUDENCE AS AN INSTRUMENT OF SOCIAL CHANGE: The Privacy Merchants: What Is To Be Done?, Amitai Etzioni\*

547. Copyright (c) 2012 University of Pennsylvania Journal of Constitutional Law University of Pennsylvania Journal of Constitutional Law, March, 2012, University of Pennsylvania Journal of Constitutional Law, 14 U. Pa. J. Const. L. 953, 17217 words, SYMPOSIUM: PRIVACY JURISPRUDENCE AS AN INSTRUMENT OF SOCIAL CHANGE: Constitutionalizing Informational Privacy by Assumption, Mary D. Fan\*

548. Copyright (c) 2012 University of Pennsylvania Journal of Constitutional Law University of Pennsylvania Journal of Constitutional Law, March, 2012, University of Pennsylvania Journal of Constitutional Law, 14 U. Pa. J. Const. L. 989, 19269 words, SYMPOSIUM: PRIVACY JURISPRUDENCE AS AN INSTRUMENT OF SOCIAL CHANGE: Bridging the Gap Between Privacy and Design+, Deirdre K. Mulligan\* and Jennifer King\*\*

549. Copyright (c) 2012 University of Pennsylvania Journal of Constitutional Law University of Pennsylvania Journal of Constitutional Law, March, 2012, University of Pennsylvania Journal of Constitutional Law, 14 U. Pa. J. Const. L. 1035, 21344 words, SYMPOSIUM: PRIVACY JURISPRUDENCE AS AN INSTRUMENT OF SOCIAL CHANGE: Fighting on a New Battlefield Armed with Old Laws: How to Monitor Terrorism in the Virtual World+, Lisa Ugelow\* and Lance J. Hoffman\*\*

550. Copyright (c) 2012 University of Pennsylvania Journal of Constitutional Law University of Pennsylvania Journal of Constitutional Law, March, 2012, University of Pennsylvania Journal of Constitutional Law, 14 U. Pa. J. Const. L. 1077, 10850 words, SYMPOSIUM: PRIVACY JURISPRUDENCE AS AN INSTRUMENT OF SOCIAL CHANGE: Reframing Privacy 2.0 in Online Social Networks, Heng Xu\*

551. Copyright (c) 2011 University of Pennsylvania Journal of Constitutional Law University of Pennsylvania Journal of Constitutional Law, May, 2011, University of Pennsylvania Journal of Constitutional Law, 13 U. Pa. J. Const. L. 1115, 11830 words, COMMENT: Plea Bargaining for DNA: Implications on the Right to Privacy, Linda Bartusiak\*

552. www.law.upenn.edu/journals/lawreview/ Copyright (c) 2014 University of Pennsylvania Law Review University of Pennsylvania Law Review, January, 2014, University of Pennsylvania Law Review, 162 U. Pa. L. Rev. 373, 21900 words, ARTICLE: THE NEXT GENERATION COMMUNICATIONS PRIVACY ACT, Orin S. Kerr+

553. www.law.upenn.edu/journals/lawreview/ Copyright (c) 2013 University of Pennsylvania Law Review University of Pennsylvania Law Review, May, 2013, University of Pennsylvania Law Review, 161 U. Pa. L. Rev. 1623, 19994 words, ARTICLE: INFORMATION PRIVACY IN THE CLOUD, Paul M. Schwartz+

554. Copyright © 2014 The Trustees of the University of Pennsylvania University of Pennsylvania Law Review Online, 2014, University of Pennsylvania Law Review Online, 162 U. Pa. L. Rev. Online 231, 2728 words, RESPONSE: COMMUNICATIONS PRIVACY FOR AND BY WHOM?, RYAN CALO +

555. Copyright (c) 2013 Dickinson School of Law Penn State Law Review, Summer, 2013, Penn State Law Review, 118 Penn St. L. Rev. 129, 19290 words, Article: Terrorism, Tips, and the Touchstone of Reasonableness: Seeking a Balance Between Threat Response and Privacy Dilution, Geoffrey S. Corn\*

556. Copyright (c) 2010 Dickinson School of Law Penn State Law Review, Winter, 2010, PENN STATE LAW REVIEW, 114 Penn St. L. Rev. 809, 23976 words, Article: People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship, M. Ryan Calo\*

557. Copyright (c) 2013 University of Pittsburgh Journal of Technology Law & Policy University of Pittsburgh Journal of Technology Law & Policy, Spring, 2013, University of Pittsburgh Journal of Technology Law & Policy, 13 PGH. J. Tech. L. & Pol'y 1, 10513 words, ARTICLE: The New Privacy Battle: How the Expanding Use of Drones Continues to Erode Our Concept of Privacy and Privacy Rights, Chris Schlag \*

558. Copyright (c) 2012 University of Pittsburgh Journal of Technology Law & Policy University of Pittsburgh Journal of Technology Law & Policy, Spring, 2012, University of Pittsburgh Journal of Technology Law & Policy, 12 PGH. J. Tech. L. & Pol'y 2, 8864 words, ARTICLE: SMARTPHONE USAGE AND THE NEED FOR CONSUMER PRIVACY LAWS, By Laura E. Gomez-Martin

559. Copyright (c) 2010 University of Pittsburgh Journal of Technology Law & Policy University of Pittsburgh Journal of Technology Law & Policy, Spring, 2010, University of Pittsburgh Journal of Technology Law & Policy, 10 PGH. J. Tech. L. & Pol'y 1, 13665 words, ARTICLE: Google Street View: Walking the Line of Privacy- Intrusion upon Seclusion and Publicity Given to Private Facts in the Digital Age, By: Jordan E. Segall \*

560. Copyright (c) 2012 Pepperdine Journal of Business, Entreprenurship & the Law, All Rights Reserved. Pepperdine Journal of Business, Entreprenurship & the Law, 2012, Pepperdine Journal of Business, Entrepreneurship & the Law, 6 J. Bus. Entrepreneurship & L. 103, 16436 words, ARTICLE: FACEBOOK IS NOT YOUR FRIEND: PROTECTING A PRIVATE EMPLOYEE'S EXPECTATION OF PRIVACY IN SOCIAL NETWORKING CONTENT IN THE TWENTY-FIRST CENTURY WORKPLACE, Cara Magatelli\*

561. Copyright (c) 2012 Pepperdine University School of Law Pepperdine Law Review, 2012, Pepperdine Law Review, 39 Pepp. L. Rev. 701, 20659 words, COMMENT: The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy, Kyle Malone\*

562. Copyright (c) 2012 Regent University Law Review Regent University Law Review, 2012 / 2013, Regent University Law Review, 25 Regent U.L. Rev. 153, 13797 words, ARTICLE: ONLINE PRIVACY PROTECTION: PROTECTING PRIVACY, THE SOCIAL CONTRACT, AND THE RULE OF LAW IN THE VIRTUAL WORLD, Matthew Sundquist\*

563. Copyright (c) 2010 The University of Texas School of Law The Review of Litigation, Summer, 2010, The Review of Litigation, 29 Rev. Litig. 895, 15131 words, ARTICLE: Wake-Up Call: Striking a Balance Between Privacy Rights and Institutional Liability in the Student Suicide Crisis, Kelley Kalchthaler

564. Copyright (c) 2009 Universidad Interamericana de Puerto Rico Revista Juridica de la Universidad Interamericana de Puerto Rico, August - May, 2009-2010, Revista Juridica Universidad Interamericana De Puerto Rico Facultad De Derecho, 44 Rev. Jur. U.I.P.R. 383, 10928 words, ARTICLE: DO DEFENDANTS HAVE A PRIVACY INTEREST IN THEIR CELL PHONE'S TEXT MESSAGES AND E-MAILS?, Juan A. Albino \*

565. Copyright (c) 2011 T.C. Williams School of Law University of Richmond Richmond Journal of Law & Technology, Fall, 2011, Richmond Journal of Law & Technology, 18 Rich. J.L. & Tech. 1, 11719 words, ARTICLE: CURRENT AND EMERGING TRANSPORTATION TECHNOLOGY: FINAL NAILS IN THE COFFIN OF THE DYING RIGHT OF PRIVACY?, By James D. Phillips \* and Katharine E. Kohm \*\*

566. Copyright (c) 2011 T.C. Williams School of Law University of Richmond Richmond Journal of Law & Technology, Spring, 2011, Richmond Journal of Law & Technology, 17 Rich. J.L. & Tech. 12, 26760 words, ARTICLE: RETHINKING REASONABLE EXPECTATIONS OF PRIVACY IN ONLINE SOCIAL NETWORKS, By Bryce Clayton Newell \*

567. Copyright (c) 2011 T.C. Williams School of Law University of Richmond Richmond Journal of Law & Technology, Spring, 2011, Richmond Journal of Law & Technology, 17 Rich. J.L. & Tech. 13, 21856 words, ARTICLE: BETTER LATE THAN NEVER: HOW THE ONLINE ADVERTISING INDUSTRY'S RESPONSE TO PROPOSED PRIVACY LEGISLATION ELIMINATES THE NEED FOR REGULATION, By Catherine Schmierer \*

568. Copyright (c) 2011 T.C. Williams School of Law University of Richmond Richmond Journal of Law & Technology, Spring, 2011, Richmond Journal of Law & Technology, 17 Rich. J.L. & Tech. 14, 12672 words, ARTICLE: RE-MAPPING PRIVACY LAW: HOW THE GOOGLE MAPS SCANDAL REQUIRES TORT LAW REFORM, By Lindsey A. Strachan

569. Copyright (c) 2013 Rutgers Computer and Technology Law Journal Rutgers Computer and Technology Law Journal, 2013, Rutgers Computer and Technology Law Journal, 39 Rutgers Computer & Tech. L.J. 56, 16726 words, NOTE & COMMENT: WHY-SPY? AN ANALYSIS OF PRIVACY AND GEOLOCATION IN THE WAKE OF THE 2010 GOOGLE "WI-SPY" CONTROVERSY, Raymond Chow\*

570. Copyright (c) 2013 Rutgers School of Law-Camden Rutgers Law Journal, Spring / Summer, 2013, Rutgers Law Journal, 43 Rutgers L. J. 725, 7533 words, TWENTY-FOURTH ISSUE ON STATE CONSTITUTIONAL LAW: STATE CONSTITUTIONAL LAW: STATE CONSTITUTIONAL LAW--PRIVACY--SEARCH AND SEIZURE--DO INDIVIDUALS HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR CELL PHONE CONVERSATIONS? STATE v. ALLEN, 241 P.3D 1045 (Mont. 2010)., Jason D. Lerner\*

571. Copyright (c) 2011 Rutgers School of Law-Camden Rutgers Law Journal, Spring, 2011, Rutgers Law Journal, 42 Rutgers L. J. 765, 10629 words, NOTE: RELATIONAL PRIVACY--A RIGHT TO GRIEVE IN THE INFORMATION AGE: HALTING THE DIGITAL DISSEMINATION OF DEATH-SCENE IMAGES, Christine M. Emery \*

572. Copyright (c) 2010 Rutgers School of Law-Camden Rutgers Law Journal, Summer, 2010, Rutgers Law Journal, 41 Rutgers L. J. 993, 5677 words, STATE CONSTITUTIONAL LAW: DEVELOPMENTS IN STATE CONSTITUTIONAL LAW: 2009: STATE CONSTITUTIONAL LAW-RIGHT OF PRIVACY- CITIZENS' RIGHT TO FLY HIGH NOT YET RIPE FOR REVIEW ACCORDING TO ALASKA SUPREME COURT. STATE v. AMERICAN CIVIL LIBERTIES UNION OF ALASKA, 204 P.3D 364 (ALASKA 2009)., Zoha Barkeshli\*

573. Copyright (c) 2010 Rutgers School of Law-Camden Rutgers Law Journal, Summer, 2010, Rutgers Law Journal, 41 Rutgers L. J. 1009, 7789 words, STATE CONSTITUTIONAL LAW: DEVELOPMENTS IN STATE CONSTITUTIONAL LAW: 2009: STATE CONSTITUTIONAL LAW-SEARCH AND SEIZURE-DO INDIVIDUALS HAVE A REASONABLE EXPECTATION OF PRIVACY IN THE CONTENTS OF THEIR TRASH? BAREKMAN v. STATE, 200 P.3D 802 (WYO. 2009), Keith S. Carmy\*

574. Copyright (c) 2013 Rutgers University, The State University of New Jersey Rutgers Law Review, Summer, 2013, Rutgers Law Review, 65 Rutgers L. Rev. 951, 7954 words, SYMPOSIUM 2013: WHERE THERE IS NO DARKNESS: TECHNOLOGY AND THE FUTURE OF PRIVACY: INTRODUCTION: The Eternally Young Fourth Amendment Common Law, George C. Thomas III\*

575. Copyright (c) 2013 Rutgers University, The State University of New Jersey Rutgers Law Review, Summer, 2013, Rutgers Law Review, 65 Rutgers L. Rev. 965, 9865 words, SYMPOSIUM 2013: WHERE THERE IS NO DARKNESS: TECHNOLOGY AND THE FUTURE OF PRIVACY: SPEECH: Symposium Keynote Address, Jeffrey Rosen\*

576. Copyright (c) 2013 Rutgers University, The State University of New Jersey Rutgers Law Review, Summer, 2013, Rutgers Law Review, 65 Rutgers L. Rev. 983, 5284 words, SYMPOSIUM 2013: WHERE THERE IS NO DARKNESS: TECHNOLOGY AND THE FUTURE OF PRIVACY: SPEECH: Tiny Constables in the Mosaic: Modernizing Oversight of Surveillance in the Age of Big Data, H. Bryan Cunningham\*

577. Copyright (c) 2013 Rutgers University, The State University of New Jersey Rutgers Law Review, Summer, 2013, Rutgers Law Review, 65 Rutgers L. Rev. 995, 17103 words, SYMPOSIUM 2013: WHERE THERE IS NO DARKNESS: TECHNOLOGY AND THE FUTURE OF PRIVACY: ARTICLE: Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements, Clifford S. Fishman\*

578. Copyright (c) 2013 Rutgers University, The State University of New Jersey Rutgers Law Review, Summer, 2013, Rutgers Law Review, 65 Rutgers L. Rev. 1041, 29198 words, SYMPOSIUM 2013: WHERE THERE IS NO DARKNESS: TECHNOLOGY AND THE FUTURE OF PRIVACY: ARTICLE: Pass Parallel Privacy Standards or Privacy Perishes, Anne T. McKenna\*

579. Copyright (c) 2010 Rutgers University, The State University of New Jersey Rutgers Law Review, Summer, 2010, Rutgers Law Review, 62 Rutgers L. Rev. 993, 15172 words, NOTE: Curiouser and Curiouser: Are Employers the Modern Day Alice in Wonderland? Closing the Ambiguity in Federal Privacy Law as Employers Cyber-Snoop Beyond the Workplace, Cicero H. Brabham, Jr.\*

580. Copyright (c) 2011 St. John's Law Review Ass'n. St. John's Law Review, Winter, 2011, St. John's Law Review, 85 St. John's L. Rev. 313, 21589 words, NOTE: FERES AND THE PRIVACY ACT: ARE MILITARY PERSONNEL RECORDS PROTECTED?, Eric Juergens+

581. Copyright (c) 2011 Saint Louis University School of Law Saint Louis University Law Journal, Spring, 2011, Saint Louis University Law Journal, 55 St. Louis L.J. 1047, 19352 words, ARTICLE: UNDERMINED NORMS: THE CORROSIVE EFFECT OF INFORMATION PROCESSING TECHNOLOGY ON INFORMATIONAL PRIVACY, RICHARD WARNER\*

582. Copyright (c) 2012 St. Thomas Law Review St. Thomas Law Review, Fall, 2012, St. Thomas Law Review, 25 St. Thomas L. Rev. 1, 8200 words, GENERAL ISSUE: LECTURE: ST. THOMAS UNIVERSITY SCHOOL OF LAW, FALL 2012: DISTINGUISHED SPEAKER SERIES FEATURED SELECTION: WHAT MUST WE HIDE: THE ETHICS OF PRIVACY AND THE ETHOS OF DISCLOSURE, Anita L. Allen\*

583. Copyright (c) 2013 St. Thomas Law Review St. Thomas Law Review, Summer, 2013, St. Thomas Law Review, 25 St. Thomas L. Rev. 335, 10804 words, 25TH ANNIVERSARY ISSUE: ARTICLE: SOCIAL MEDIA IN THE SUNSHINE: DISCOVERY AND ETHICS OF SOCIAL MEDIA - FLORIDA'S RIGHT TO PRIVACY SHOULD CHANGE THE ANALYSIS, Spencer Kuvin\* and Chelsea Silvia\*\*

584. Copyright (c) 2012 St. Thomas Law Review St. Thomas Law Review, Spring, 2012, St. Thomas Law Review, 24 St. Thomas L. Rev. 169, 43557 words, CRIMINAL LAW ISSUE: FEATURED CONTRIBUTOR: SURVEILLANCE TECHNOLOGY AND THE LOSS OF SOMETHING A LOT LIKE PRIVACY: AN EXAMINATION OF THE "MOSAIC THEORY" AND THE LIMITS OF THE FOURTH AMENDMENT, Courtney E. Walsh n1

585. Copyright (c) 2013 San Diego International Law Journal San Diego International Law Journal, Spring, 2013, San Diego International Law Journal, 14 San Diego Int'l L.J. 281, 21951 words, COMMENT: Drawing the Line Between Competing Interests: Strengthening Online Data Privacy Protection in an Increasingly Networked World, LORI CHIU\*

586. Copyright (c) 2010 San Diego International Law Journal San Diego International Law Journal, Fall, 2010, San Diego International Law Journal, 12 San Diego Int'l L.J. 263, 18532 words, COMMENT: Reinforcing the Hague Convention on Taking Evidence Abroad After Blocking Statutes, Data Privacy Directives, and Aerospatiale, BRIAN FRIEDERICH\*

587. Copyright (c) 2011 San Diego Law Review Association San Diego Law Review, August / September, 2011, San Diego Law Review, 48 San Diego L. Rev. 809, 20194 words, ARTICLE: The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption ofBest Practices, ANDREW SERWIN\*

588. Copyright (c) 2012 University of San Francisco School of Law University of San Francisco Law Review, Fall, 2012, University of San Francisco Law Review, 47 U.S.F. L. Rev. 225, 9614 words, SYMPOSIUM: Big Brother in the 21st Century?: Reforming the Electronic Communications Privacy Act: Speech: Keynote Address: The Path to ECPA Reform and the Implications of United States v. Jones, By James X. Dempsey\*

589. Copyright (c) 2012 University of San Francisco School of Law University of San Francisco Law Review, Fall, 2012, University of San Francisco Law Review, 47 U.S.F. L. Rev. 245, 4823 words, SYMPOSIUM: Big Brother in the 21st Century?: Reforming the Electronic Communications Privacy Act: Speech: Mapping Our Privacy: The Use and Misuse of Location Data (A Law Enforcement Perspective and Legislative Balancing), By Stephanie K. Pell\*

590. Copyright (c) 2012 University of San Francisco School of Law University of San Francisco Law Review, Fall, 2012, University of San Francisco Law Review, 47 U.S.F. L. Rev. 257, 6270 words, SYMPOSIUM: Big Brother in the 21st Century?: Reforming the Electronic Communications Privacy Act: Article: Standing Up for Mr. Nesbitt, By Stephen Wm. Smith\*

591. Copyright (c) 2012 University of San Francisco School of Law University of San Francisco Law Review, Fall, 2012, University of San Francisco Law Review, 47 U.S.F. L. Rev. 269, 10423 words, SYMPOSIUM: Big Brother in the 21st Century?: Reforming the Electronic Communications Privacy Act: Article: Electronic Surveillance Law and the Intra-Agency Separation of Powers, By Paul Ohm\*

592. Copyright (c) 2012 University of San Francisco School of Law University of San Francisco Law Review, Fall, 2012, University of San Francisco Law Review, 47 U.S.F. L. Rev. 291, 23158 words, SYMPOSIUM: Big Brother in the 21st Century?: Reforming the Electronic Communications Privacy Act: Article: Caution Advised: Avoid Undermining the Legitimate Needs of Law Enforcement to Solve Crimes Involving the Internet in Amending the Electronic Communications Privacy Act, By Kevin V. Ryan and Mark L. Krotoski\*

593. Copyright (c) 2012 University of San Francisco School of Law University of San Francisco Law Review, Fall, 2012, University of San Francisco Law Review, 47 U.S.F. L. Rev. 353, 12267 words, Comment: Trolling Attacks and the Need for New Approaches to Privacy Torts, By Arthur Gaus\*

594. Copyright (c) 2010 University of San Francisco School of Law University of San Francisco Law Review, Spring, 2010, University of San Francisco Law Review, 44 U.S.F. L. Rev. 907, 12647 words, Comment: Consumer Credit Reports and Privacy in the Employment Context: The Fair Credit Reporting Act and the Equal Employment for All Act, By Ruth Desmond\*

595. Copyright (c) 2013 Santa Clara Computer & High Technology Law Journal Santa Clara High Technology Law Journal, December, 2013, Santa Clara High Technology Law Journal, 30 Santa Clara Computer & High Tech. L.J. 57, 14715 words, ARTICLE: HERE, THERE AND EVERYWHERE: MOBILITY DATA IN THE EU (HELP NEEDED: WHERE IS PRIVACY?), Raffaele Zallone+

596. Copyright (c) 2012 Santa Clara Computer & High Technology Law Journal Santa Clara Computer & High Technology Law Journal, 2012 - 2013, Santa Clara Computer & High Technology Law Journal, 29 Santa Clara Computer & High Tech. L.J. 165, 16624 words, ARTICLE: TURNING A NEW LEAF: A PRIVACY ANALYSIS OF CARWINGS ELECTRIC VEHICLE DATA COLLECTION AND TRANSMISSION, Francesca Svarcas+

597. Copyright (c) 2012 Santa Clara Computer & High Technology Law Journal Santa Clara Computer & High Technology Law Journal, 2012 / 2013, Santa Clara Computer & High Technology Law Journal, 29 Santa Clara Computer & High Tech. L.J. 451, 16824 words, ARTICLE: THE INFORMATION PRIVACY LAW OF WEB APPLICATIONS AND CLOUD COMPUTING, Sebastian Zimmeck+

598. Copyright (c) 2011 Santa Clara Computer & High Technology Law Journal Santa Clara Computer & High Technology Law Journal, 2011 - 2012, Santa Clara Computer & High Technology Law Journal, 28 Santa Clara Computer & High Tech. L.J. 743, 12205 words, SYMPOSIUM REVIEW: HOW CONCEPCION KILLED THE PRIVACY CLASS ACTION, Jessica L. Hubley+

599. Copyright (c) 2011 Santa Clara Computer & High Technology Law Journal Santa Clara Computer & High Technology Law Journal, February, 2011, Santa Clara Computer & High Technology Law Journal, 27 Santa Clara Computer & High Tech. L.J. 3, 31926 words, ARTICLE: BALANCING CONSUMER PRIVACY WITH BEHAVIORAL TARGETING, Dustin D. Berger+

600. Copyright (c) 2011 Santa Clara Computer & High Technology Law Journal Santa Clara Computer & High Technology Law Journal, February, 2011, Santa Clara Computer & High Technology Law Journal, 27 Santa Clara Computer & High Tech. L.J. 63, 30586 words, ARTICLE: CONTEXTUALIZING THE TENSIONS AND WEAKNESSES OF INFORMATION PRIVACY AND DATA BREACH NOTIFICATION LAWS, Mark Burdon+

601. Copyright (c) 2011 Santa Clara Computer & High Technology Law Journal Santa Clara Computer & High Technology Law Journal, February, 2011, Santa Clara Computer & High Technology Law Journal, 27 Santa Clara Computer & High Tech. L.J. 175, 24193 words, ARTICLE: UPHOLDING FREE SPEECH AND PRIVACY ONLINE: A LEGAL-BASED AND MARKET-BASED APPROACH FOR INTERNET COMPANIES IN CHINA, Yutian Ling+

602. Copyright (c) 2011 Santa Clara Computer & High Technology Law Journal Santa Clara Computer & High Technology Law Journal, February, 2011, Santa Clara Computer & High Technology Law Journal, 27 Santa Clara Computer & High Tech. L.J. 219, 13668 words, 2010 COMMENT CONTEST WINNER: BALANCING INTERESTS AT THE BORDER: PROTECTING OUR NATION AND OUR PRIVACY IN BORDER SEARCHES OF ELECTRONIC DEVICES, Carolyn James+

603. Copyright (c) 2014 School of Law, Santa Clara University Santa Clara Law Review, 2014, Santa Clara Law Review, 54 Santa Clara L. Rev. 497, 14200 words, COMMENT: THE UNCERTAIN FUTURE: PRIVACY AND SECURITY IN CLOUD COMPUTING, James Ryan\*

604. Copyright (c) 2012 School of Law, Santa Clara University Santa Clara Law Review, 2012, Santa Clara Law Review, 52 Santa Clara L. Rev. 1157, 4804 words, SYMPOSIUM ARTICLE: "But Officer, it wasn't my fault ... the car did it!": CRIMINAL LIABILITY ISSUES CREATED BY AUTONOMOUS VEHICLES, Frank Douma\* and Sarah Aue Palodichuk\*\*

... may fall on the shoulders of the car owners rather than drivers; **privacy,** such as what information the car will provide for enforcement purposes; ...

605. Copyright (c) 2012 School of Law, Santa Clara University Santa Clara Law Review, 2012, Santa Clara Law Review, 52 Santa Clara L. Rev. 1171, 27231 words, SYMPOSIUM ARTICLE: PRIVACY IN AUTONOMOUS VEHICLES, Dorothy J. Glancy\*

**Privacy and privacy** laws will significantly influence the development of autonomous vehicles. ...

... individual person with an autonomous vehicle brings a number of **privacy** interests into play. Autonomy **privacy** interests, personal information **privacy** interestsand surveillance **privacy** interests will all affect the powerful disruptive technologies involved in autonomous vehicles. Each of these **privacy** interests is associated with a substantial body of **privacy** law that will apply to autonomous vehicles. Because different configurations of autonomous vehicles will affect the reasonableness of **privacy** expectations regarding autonomous vehicles, this Article uses two ...

... understanding some of the ways in which autonomous vehicles will affect **privacy** at the same time as **privacy** affects autonomous vehicles. Autonomous vehicles will impact the ...

... adopt potential strategies for optimizing interactions between **privacy** andautonomous vehicles.

606. Copyright (c) 2012 School of Law, Santa Clara University Santa Clara Law Review, 2012, Santa Clara Law Review, 52 Santa Clara L. Rev. 1423, 29100 words, SYMPOSIUM ARTICLE: THE POTENTIAL REGULATORY CHALLENGES OF INCREASINGLY AUTONOMOUS MOTOR VEHICLES n1, Stephen P. Wood,\* Jesse Chang,\*\* Thomas Healy\*\*\* and John Wood\*\*\*\*

... about issues such as accuracy, timeliness, interoperability, cyber security, **privacy** and public acceptance. In this Article, we examine how NHTSA's ...

607. Copyright (c) 2013 The Seattle University Law Review Seattle University Law Review, Spring, 2013, Seattle University Law Review, 36 Seattle Univ. L. R. 1553, 10338 words, NOTE: Public Duties, Private Rights: Privacy and Unsubstantiated Allegations in Washington's Public Records Act, Robert E. Miller \*

608. Copyright (c) 2011 The Seattle University Law Review Seattle University Law Review, Winter, 2011, Seattle University Law Review, 34 Seattle Univ. L. R. 439, 21602 words, ARTICLE: The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?, Dennis D. Hirsch +

609. Copyright (c) 2010 Seton Hall Journal of Sports and Entertainment Law Journal of Sports and Entertainment Law, 2010, Journal of Sports and Entertainment Law, 20 Seton Hall J. Sports & Ent. L. 227, 8699 words, ARTICLE: DOES ANTI-PAPARAZZI MEAN ANTI-PRESS?: FIRST AMENDMENT IMPLICATIONS OF PRIVACY LEGISLATION FOR THE NEWSROOM, Christina M. Locke\*

610. Copyright (c) 2010 Seton Hall University School of Law Seton Hall Law Review, 2010, Seton Hall Law Review, 40 Seton Hall L. Rev. 1257, 19470 words, COMMENT: A Break in the Internet Privacy Chain: How Law Enforcement Connects Content to Non-Content to Discover an Internet User's Identity, Laura J. Tyson\*

611. Copyright (c) 2012 Chicago-Kent College of Law, All Rights Reserved. The Seventh Circuit Review, Spring, 2012, The Seventh Circuit Review, 7 Seventh Circuit Rev. 126, 15533 words, PRIVACY: THAT'S THE TICKET: ARGUING FOR A NARROWER INTERPRETATION OF THE EXCEPTIONS CLAUSE IN THE DRIVER'S PRIVACY PROTECTION ACT, KATHERINE HUTCHISON \*

612. Copyright (c) 2013 South Carolina Law Review South Carolina Law Review, Winter, 2013, South Carolina Law Review, 65 S.C. L. Rev. 373, 22613 words, ARTICLE: THE SURVEILLANCE SOCIETY AND THE THIRD-PARTY PRIVACY PROBLEM, Shaun B. Spencer \*

613. Copyright (c) 2013 South Carolina Law Review South Carolina Law Review, Spring, 2013, South Carolina Law Review, 64 S.C. L. Rev. 717, 18531 words, ARTICLE: BLEEDING DATA IN A POOL OF SHARKS: THE ANATHEMA OF PRIVACY IN A WORLD OF DIGITAL SHARING AND ELECTRONIC DISCOVERY, Derek S. Witte \*

614. Copyright (c) 2011 South Carolina Law Review South Carolina Law Review, Summer, 2011, South Carolina Law Review, 62 S.C. L. Rev. 671, 11794 words, CRIMINAL PROCEDURE: ARTICLE: Who Has More Privacy?: State v. Brown and Its Effect on South Carolina Criminal Defendants, Jaclyn L. McAndrew

615. Copyright (c) 2014 South Dakota Law Review South Dakota Law Review, 2014, South Dakota Law Review, 59 S.D. L. REV. 35, 8014 words, ARTICLE: PRIVACY IN THE WORKPLACE, FACT OR FICTION, AND THE VALUE OF AN AUTHORIZED USE POLICY (AUP), GREGORY M. HUCKABEE+ and CHERRY KOLB+

616. Copyright (c) 2012 South Dakota Law Review South Dakota Law Review, 2012, South Dakota Law Review, 57 S.D. L. REV. 1, 3678 words, ARTICLE: MEDICAL PRIVACY: THE SOUTH DAKOTA SUPREME COURT ADOPTS SDCL 19-2-13, James D. Leach+

617. Copyright (c) 2010 South Dakota Law Review South Dakota Law Review, 2010, South Dakota Law Review, 55 S.D. L. REV. 299, 18135 words, STUDENT ARTICLE: ARIZONA V. GANT: HEIGHTENING A PERSON'S EXPECTATION OF PRIVACY IN A MOTOR VEHICLE FOLLOWING SEARCHES INCIDENT TO ARREST, Jeffrey R. Beck+

618. Copyright (c) 2014 Gould School of Law Southern California Interdisciplinary Law Journal, Winter, 2014, Southern California Interdisciplinary Law Journal, 23 S. Cal. Interdis. L.J. 409, 19405 words, NOTE: IS THE COURT ALLERGIC TO KATZ? PROBLEMS POSED BY NEW METHODS OF ELECTRONIC SURVEILLANCE TO THE "REASONABLE-EXPECTATION-OF-PRIVACY" TEST, Colin Shaff\*

619. Copyright (c) 2012 Gould School of Law Southern California Interdisciplinary Law Journal, Winter, 2012, Southern California Interdisciplinary Law Journal, 21 S. Cal. Interdis. L.J. 359, 23191 words, NOTE: UNWARRANTED! PRIVACY IN A TECHNOLOGICAL AGE: THE FOURTH AMENDMENT DIFFICULTY IN PROTECTING AGAINST WARRANTLESS GPS TRACKING AND THE SUBSTANTIVE DUE PROCESS AND FIRST AMENDMENT BOOST, Courtney Burten\*

620. Copyright (c) 2010 Gould School of Law Southern California Interdisciplinary Law Journal, Winter, 2010, SOUTHERN CALIFORNIA INTERDISCIPLINARY LAW JOURNAL, 19 S. Cal. Interdis. L.J. 353, 21361 words, NOTE: SIX-FIGURE BOOK DEALS, CELEBRITY FAME, AND A SPREAD IN PLAYBOY n1: FREE SPEECH AND PRIVACY CONCERNS IN THE BLOGOSPHERE, Autumn E. Love\*

621. Copyright (c) 2013 University of Southern California Southern California Law Review, November, 2013, Southern California Law Review, 87 S. Cal. L. Rev. 1, 28723 words, ARTICLE: PRIVACY, THE HACKER WAY, Andrea M. Matwyshyn\*

622. Copyright (c) 2010 University of Southern California Southern California Law Review, November, 2010, Southern California Law Review, 84 S. Cal. L. Rev. 201, 23994 words, NOTE: TAMING THE PAPARAZZI IN THE "WILD WEST": A LOOK AT CALIFORNIA'S 2009 AMENDMENT TO THE ANTI-PAPARAZZI ACT AND A CALL FOR INCREASED PRIVACY PROTECTIONS FOR CELEBRITY CHILDREN, Lauren N. Follett\*

623. Copyright (c) 2014 University of Southern California Southern California Law Review Postscript, 2014, Southern California Law Review Postscript, 87 S. Cal. L. Rev. 1A, 14476 words, ARTICLE: KEEPING TRACK OF THE JONESES: REDEFINING THE PRIVACY BOUNDARIES OF THE DIGITAL AGE, KEVIN KROLL \*

624. Copyright (c) 2014 University of Southern California Southern California Law Review Postscript, 2014, Southern California Law Review Postscript, 78 S. Cal. L. Rev. 120A, 10581 words, ARTICLE: TRAVELING TRANSGENDER: HOW AIRPORT SCREENING PROCEDURES THREATEN THE RIGHT TO INFORMATIONAL PRIVACY, DEEMA B. ABINI \*

625. Copyright (c) 2012 Southern Methodist University SMU Law Review, Winter, 2012, SMU Law Review, 65 SMU L. Rev. 85, 35477 words, ARTICLE: Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research, Sharona Hoffman\* and Andy Podgurski\*\*

626. Copyright (c) 2011 Southern Methodist University SMU Law Review, Fall, 2011, SMU Law Review, 64 SMU L. Rev. 1433, 18042 words, COMMENT: Privacy's Role in the Discovery of Social Networking Site Information, Kelly Ann Bub\*

627. Copyright (c) 2011 SMU Dedman School of Law SMU Science & Technology Law Review, Fall, 2011, SMU Science & Technology Law Review, 15 SMU Sci. & Tech. L. Rev. 101, 5727 words, CASE NOTE: Paying for Privacy: An Unjust Facade, Scott M. Ruggiero\*

628. Copyright (c) 2011 SMU Dedman School of Law SMU Science & Technology Law Review, Summer, 2011, SMU Science & Technology Law Review, 14 SMU Sci. & Tech. L. Rev. 365, 16176 words, SELECTED MATERIAL FROM 2011 GAME::BUSINESS::LAW INTERNATIONAL SUMMIT ON THE LAW AND BUSINESS OF VIDEO GAMES: Privacy: Problems and Solutions, Moderator: Professor Xuan-Thao Nguyen, SMU Dedman School of Law Panelists: Jennifer Archie, Partner, Latham & Watkins LLP, Andrew S. Ehmke, Partner, Haynes and Boone, LLP, Dr. Joshua Fairfield, Washington & Lee School of Law and Berin Szoka, Founder, TechFreedom

629. Copyright (c) 2012 Southern University Law Review Southern University Law Review, Spring, 2012, Southern University Law Review, 39 S.U. L. Rev. 243, 10819 words, ARTICLE: PRIVACY IS DEAD: THE BIRTH OF SOCIAL MEDIA BACKGROUND CHECKS, Sherry D. Sanders\*

630. Copyright (c) 2010 by Southwestern Law School Southwestern Journal of International Law, 2010, SOUTHWESTERN JOURNAL OF INTERNATIONAL LAW, 16 Sw. J. Int'l L. 131, 14009 words, ARTICLE: MEDICAL PRIVACY AND LITIGATION DISCOVERY: CAN THEY BE HARMONIZED? THE AMERICAN AND CANADIAN PERSPECTIVES, Hillary Levun\*

631. Copyright (c) 2012 Southwestern Law School Southwestern Law Review, 2012, Southwestern Law Review, 42 Sw. L. Rev. 263, 15925 words, ARTICLE: LOCATIONAL PRIVACY IN THE SKY: PROTECTING THE MOVEMENTS OF NON-COMMERCIAL AIRCRAFT FROM PUBLIC VIEW, Trevor Roe\*

632. Copyright (c) 2010 Southwestern Law School Southwestern Law Review, 2010, Southwestern Law Review, 39 Sw. L. Rev. 433, 28204 words, ARTICLE: FINANCIAL DISCLOSURE ON DEATH OR DIVORCE: BALANCING PRIVACY OF INFORMATION WITH PUBLIC ACCESS TO THE COURTS, Donna Litman\*

633. Copyright (c) 2014 Board of Trustees of the Leland Stanford Junior University Stanford Journal of International Law, Winter, 2014, Stanford Journal of International Law, 50 Stan. J Int'l L. 53, 26655 words, ARTICLE: The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses, Dan Jerker B. Svantesson\*

634. Copyright (c) 2011 The Board of Trustees of Leland Stanford Junior University Stanford Law Review, January, 2011, Stanford Law Review, 63 Stan. L. Rev. 247, 32722 words, ARTICLE: Privacy on the Books and on the Ground, Kenneth A. Bamberger\* and Deirdre K. Mulligan\*\*

635. Copyright (c) 2012 Board of Trustees of the Leland Stanford Junior University Stanford Technology Law Review, 2012, Stanford Technology Law Review, 2012 Stan. Tech. L. Rev. 7, 7980 words, ARTICLE: Social Media Privacy: A Dozen Myths and Facts, LOTHAR DETERMANN \*

636. Copyright (c) 2013 Board of Trustees of the Leland Stanford Junior University Stanford Technology Law Review, Winter, 2013, Stanford Technology Law Review, 16 Stan. Tech. L. Rev. 369, 28609 words, ARTICLE: IT'S ABOUT TIME: PRIVACY, INFORMATION LIFE CYCLES, AND THE RIGHT TO BE FORGOTTEN, Meg Leta Ambrose \*

637. Copyright (c) 2012 Suffolk University Suffolk Transnational Law Review, Summer, 2012, Suffolk Transnational Law Review, 35 Suffolk Transnat'l L. Rev. 363, 11071 words, NOTE: UNTANGLING THE WEB: AN ARGUMENT FOR COMPREHENSIVE DATA PRIVACY LEGISLATION IN THE UNITED STATES, Amanda C. Border

638. Copyright (c) 2012 Suffolk University Suffolk University Law Review, 2012, Suffolk University Law Review, 45 Suffolk U. L. Rev. 1177, 19107 words, NOTE: Massachusetts Genetic Bill of Rights: Chipping Away at Genetic Privacy, Jaclyn G. Ambriscoe

639. Copyright (c) 2010 Suffolk University Suffolk University Law Review, 2010, Suffolk University Law Review, 43 Suffolk U. L. Rev. 957, 11946 words, NOTE: CAN-SPAM Versus the European Union E-Privacy Directive: Does Either Provide a Solution to the Problem of Spam?, Ariella Mutchler

640. Copyright (c) 2014 Syracuse Law Review Syracuse Law Review, 2014, Syracuse Law Review, 64 Syracuse L. Rev. 131, 19029 words, ARTICLE: PRIVACY AND MHEALTH: HOW MOBILE HEALTH "APPS" FIT INTO A PRIVACY FRAMEWORK NOT LIMITED TO HIPAA, Anne Marie Helm+ and Daniel Georgatos++

641. Copyright (c) 2013 Syracuse Law Review Syracuse Law Review, 2013, Syracuse Law Review, 63 Syracuse L. Rev. 399, 15499 words, SYMPOSIUM: JURISPRUDENCE AND THE BODY: TAKING THE PULSE OF HEALTH LAW: WHEN PRIVACY IS NOT AN OPTION: CODIFYING THE CONTOURS OF NECESSARY THIRD PARTIES IN EMERGENCY MEDICAL SITUATIONS, Chris Chambers Goodman+

642. Copyright (c) 2012 Syracuse University College of Law Syracuse Science & Technology Law Reporter, Spring, 2012, Syracuse Science & Technology Law Reporter, 2012 Syracuse Sci. & Tech. L. Rep. 53, 25571 words, ARTICLE: New Fronteirs of Reprogenetics: SNP Profile Collection and Banking and the Resulting Duties in Medical Malpractice, Issues in Property Rights of Genetic Materials, and Liabilities in Genetic Privacy, By Stephanie Sgambati

643. Copyright (c) 2010 Syracuse University College of Law Syracuse Science & Technology Law Reporter, Spring, 2010, Syracuse Science & Technology Law Reporter, 2010 Syracuse Sci. & Tech. L. Rep. 38, 5557 words, ARTICLE: Biometrics, Retinal Scanning, and the Right to Privacy in the 21st Century, Stephen Hoffman \*

644. Copyright (c) 2014 Syracuse University College of Law Syracuse Science & Technology Law Reporter, Spring, 2014, Syracuse Science & Technology Law Reporter, 30 Syracuse Sci. & Tech. L. Rep. 160, 6365 words, ARTICLE: I Know What You're Thinking: Brain Imaging and Mental Privacy, Edited by: Sarah Richmond, Geraint Rees, and Sarah J.L. Edwards Reviewed By: Jenna Furman

645. Copyright (c) 2012 Syracuse University College of Law Syracuse Science & Technology Law Reporter, Fall, 2012, Syracuse Science & Technology Law Reporter, 27 Syracuse Sci. & Tech. L. Rep. 1, 8828 words, ARTICLE: Cell-Site Location Data and the Right to Privacy, Jen Manso

646. Copyright (c) 2012 Syracuse University College of Law Syracuse Science & Technology Law Reporter, Fall, 2012, Syracuse Science & Technology Law Reporter, 27 Syracuse Sci. & Tech. L. Rep. 55, 25658 words, ARTICLE: New Frontiers of Reprogenetics: SNP Profile Collection and Banking and the Resulting Duties in Medical Malpractice, Issues in Property Rights of Genetic Materials, and Liabilities in Genetic Privacy, Stephanie Sgambati, J.D. n1

647. Copyright (c) 2013 Temple Journal of Science, Technology & Environmental Law Temple Journal of Science, Technology & Environmental Law, Winter, 2013, Temple Journal of Science, Technology & Environmental Law, 32 Temp. J. Sci. Tech. & Envtl. L. 211, 13916 words, ARTICLE: Does My Employer "Control" My Facebook Account?: Emerging Social Media Privacy Concerns in the Workplace, Will N. Widman\*

648. Copyright (c) 2012 Temple Journal of Science, Technology & Environmental Law Temple Journal of Science, Technology & Environmental Law, Summer, 2012, Temple Journal of Science, Technology & Environmental Law, 31 Temp. J. Sci. Tech. & Envtl. L. 149, 15930 words, NOTE AND COMMENT: FACEbook Confidential: The Privacy Implications of Facebook's Surreptitious and Exploitative Utilization of Facial Recognition Technology, Jonathan Shaw\*

649. Copyright (c) 2013 Temple University of the Commonwealth System of Higher Education Temple Law Review, Winter, 2013, Temple Law Review, 85 Temp. L. Rev. 367, 23494 words, ARTICLE: PETITIONS, PRIVACY, AND POLITICAL OBSCURITY, Rebecca Green\*

650. Copyright (c) 2012 Temple University of the Commonwealth System of Higher Education Temple Law Review, Spring, 2012, Temple Law Review, 84 Temp. L. Rev. 599, 25074 words, ARTICLE: SLOW EXPECTATIONS: HOW CHANGING EXPECTATIONS OF PRIVACY CAN ERODE FOURTH AMENDMENT PROTECTION AND A PROPOSED SOLUTION, Teri Dobbins Baxter\*

651. Copyright (c) 2013 Temple University of the Commonwealth System of Higher Education Temple Political & Civil Rights Law Review, Fall, 2013, Temple Political & Civil Rights Law Review, 23 Temp. Pol. & Civ. Rts. L. Rev. 91, 21813 words, ARTICLE: FLORIDA V. JARDINES : PRIVACY, TRESPASS, AND THE FOURTH AMENDMENT, by David Steinberg\*

652. Copyright (c) 2012 Temple University of the Commonwealth System of Higher Education Temple Political & Civil Rights Law Review, Fall, 2012, Temple Political & Civil Rights Law Review, 22 Temp. Pol. & Civ. Rts. L. Rev. 225, 19557 words, NOTE & COMMENT: THE VANISHING RIGHT TO PRIVACY: A CRITIQUE OF THE SECOND CIRCUIT'S APPROACH TO MEDICAL CONFIDENTIALITY IN MATSON V. BOARD OF EDUCATION, Paul Nordeman\*

653. Copyright (c) 2012 Tennessee Law Review Association, Inc. Tennessee Law Review, Winter, 2012, Tennessee Law Review, 79 Tenn. L. Rev. 417, 11186 words, CASE NOTE: CONSTITUTIONAL LAW-RIGHT TO PRIVACY-GOVERNMENT CONTRACT EMPLOYEES' RIGHT TO INFORMATIONAL PRIVACY, Jed Storey Crumbo

654. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1401, 18016 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: I. ACCOUNTABILITY MECHANISMS: ARTICLE: It Came from Beneath the Twilight Zone: Wiretapping and Article II Imperialism, Heidi Kitrosser\*

655. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1435, 16036 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: I. ACCOUNTABILITY MECHANISMS: ARTICLE: Deputizing Homeland Security, Jon D. Michaels\*

656. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1475, 12277 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: I. ACCOUNTABILITY MECHANISMS: ARTICLE: The Case for Stewart over Harlan on 24/7 Physical Surveillance, Afsheen John Radsan\*

657. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1501, 18402 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: I. ACCOUNTABILITY MECHANISMS: ARTICLE: Terrorism Trials and the Article III Courts After Abu Ali, Stephen I. Vladeck\*

658. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1533, 18473 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: II. CYBERSECURITY AND NETWORK OPERATIONS: ARTICLE: Cyber Warfare and Precautions Against the Effects of Attacks, Eric Talbot Jensen\*

659. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1571, 11171 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: II. CYBERSECURITY AND NETWORK OPERATIONS: ARTICLE: Sovereign Discourse on Cyber Conflict Under International Law, Sean Kanuck\*

660. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1599, 15940 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: III. FOCUS ON FISA: ARTICLE: In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance\*, Matthew A. Anzaldi\*\* & Jonathan W. Gannon\*\*\*

661. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1633, 19754 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: III. FOCUS ON FISA: ARTICLE: Programmatic Surveillance and FISA: Of Needles in Haystacks, William C. Banks\*

662. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1669, 8794 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: IV. INVESTIGATIONS: ARTICLE: The Modest Role of the Warrant Clause in National Security Investigations, Orin S. Kerr\*

663. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1685, 15246 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: IV. INVESTIGATIONS: ARTICLE: The Argument Against Technology-Neutral Surveillance Laws, Paul Ohm\*

664. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1715, 12585 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: IV. INVESTIGATIONS: ARTICLE: The Law of Homegrown (Counter)Terrorism, Samuel J. Rascoff\*

665. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1751, 7094 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: V. NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: ARTICLE: Choosing Both: Making Technology Choices at the Intersections of Privacy and Security, Alexander W. Joel\*

666. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1767, 15620 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: V. NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: ARTICLE: The Key Theory: Authenticating Decrypted Information in Litigation While Protecting Sensitive Sources and Methods, Nicholas J. Patterson\*

667. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1795, 32486 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: V. NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: ARTICLE: Mending Walls: Information Sharing After the USA PATRIOT Act, Nathan Alexander Sales\*

668. Copyright (c) 2010 Texas Law Review Association Texas Law Review, June, 2010, Texas Law Review, 88 Tex. L. Rev. 1855, 24984 words, SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: V. NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY: ARTICLE: The Right to Privacy in Light of Presidents' Programs: What Project MINARET's Admissions Reveal about Modern Surveillance of Americans, By Lisa Graves\*

669. Copyright (c) 2011 Texas Wesleyan Law Review Texas Wesleyan Law Review, Winter, 2011, Texas Wesleyan Law Review, 18 Tex. Wesleyan L. Rev. 359, 12771 words, NOTE & COMMENT: BACK WHERE YOU BELONG: INDIVIDUALS, CORPORATIONS, AND THE THIRD CIRCUIT'S REDEFINITION OF PERSONAL PRIVACY UNDER FOIA, By: Emily A. Schneider

670. Copyright (c) 2010 Texas Wesleyan Law Review Texas Wesleyan Law Review, Spring, 2010, Texas Wesleyan Law Review, 16 Tex. Wesleyan L. Rev. 477, 10215 words, COMMENT: YOUR BORING LIFE, NOW AVAILABLE ONLINE: ANALYZING GOOGLE STREET VIEW AND THE RIGHT TO PRIVACY, By Jana McGowen

671. Copyright (c) 2014 The University of Toledo The University of Toledo Law Review, Winter, 2014, The University of Toledo Law Review, 45 U. Tol. L. Rev. 377, 19712 words, NOTE & COMMENT: YOUR DIGITAL LEASH: THE INTERACTION BETWEEN CELL PHONE-BASED GPS TECHNOLOGY AND PRIVACY RIGHTS IN UNITED STATES V. SKINNER, Christopher R. Orr\*

672. Copyright (c) 2010 The University of Toledo The University of Toledo Law Review, Summer, 2010, The University of Toledo Law Review, 41 U. Tol. L. Rev. 909, 7717 words, SYMPOSIUM ARTICLE: CLIMATE CHANGE AND THE FUTURE OF ENERGY: PRIVACY AND SMART GRID: WHEN PROGRESS AND PRIVACY COLLIDE, Kevin L. Doran\*

673. Copyright (c) 2013 Touro College Jacob D. Fuchsberg Law Center Touro Law Review, 2013, Touro Law Review, 29 Touro L. Rev. 1151, 11111 words, FOURTH AMENDMENT BODILY SEARCHES AND DNA: The Blueprint: Critiques of the Fingerprint and Abandonment Paradigms Utilized to Reject an Expectation of Privacy in DNA: Criminal Court of New York, New York City People v. Vernon B. n1 (decided June 15, 2012), Avi Goldstein\*

674. Copyright (c) 2013 Touro College Jacob D. Fuchsberg Law Center Touro Law Review, 2013, Touro Law Review, 29 Touro L. Rev. 1241, 12375 words, FOURTH AMENDMENT AND MODERNIZED SOCIETY: Fourth Amendment Right to Privacy with Respect to Bank Records in Criminal Cases: Supreme Court of New York, New York County People v. Lomma n1 (decided February 1, 2012), Francesca M. Brancato

675. Copyright (c) 2013 Touro College Jacob D. Fuchsberg Law Center Touro Law Review, 2013, Touro Law Review, 29 Touro L. Rev. 1263, 11046 words, FOURTH AMENDMENT AND MODERNIZED SOCIETY: It's Reasonable to Expect Privacy when Watching Adult Videos: Supreme Court of New York, New York County People v. Hemmings n1 (decided January 12, 2012), Matthew Leonhardt\*

676. Copyright (c) 2013 Touro College Jacob D. Fuchsberg Law Center Touro Law Review, 2013, Touro Law Review, 29 Touro L. Rev. 1283, 11433 words, FOURTH AMENDMENT AND MODERNIZED SOCIETY: Privacy in Social Media: To Tweet or Not to Tweet?: Court of Appeals of New York, People v. Harris n1 (decided June 30, 2012), Tara M. Breslawski\*

677. Copyright (c) 2012 Touro College Jacob D. Fuchsberg Law Center Touro Law Review, 2012, Touro Law Review, 28 Touro L. Rev. 771, 7608 words, Fourth Amendment and Automobiles: Do Automobile Passengers Have A Legitimate Expectation Of Privacy? An Analysis of Reasonable Expectation Under The Fourth Amendment Supreme Court of New York Appellate Term, Second Department, Lisa Belrose\*

678. Copyright (c) 2012 by the Transportation Law Journal Transportation Law Journal, 2012, Transportation Law Journal, 39 Transp. L. J. 97, 30044 words, Article: Intelligent Transportation Systems: Personal Data Needs and Privacy Law, Thomas Garry\*, Frank Douma\*\* and Stephen Simon\*\*\*

679. Copyright (c) 2011 Tulane University School of Law The Tulane European and Civil Law Forum, 2011, The Tulane European and Civil Law Forum, 26 Tul. Eur. & Civ. L.F. 67, 14031 words, ARTICLE: Three Milestones in the History of Privacy in the United States, Vernon Valentine Palmer\*

680. Copyright (c) 2010 Tulane Journal of International and Comparative Law Tulane Journal of International and Comparative Law, Winter, 2010, Tulane Journal of International and Comparative Law, 19 Tul. J. Int'l & Comp. L. 337, 13963 words, COMMENT: Bombing Out: Using Full-Body Imaging To Conduct Airport Searches in the United States and Europe Amidst Privacy Concerns, Etienne Lombard\*

681. Copyright (c) 2013 Tulane Journal of Technology & Intellectual Property Tulane Journal of Technology & Intellectual Property, Fall, 2013, Tulane Journal of Technology and Intellectual Property, 16 Tul. J. Tech. & Intell. Prop. 267, 9718 words, COMMENT: The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law, Alessandra Suuberg\*

682. Copyright (c) 2012 by the Tulane Law Review Association Tulane Law Review, June, 2012, Tulane Law Review, 86 Tul. L. Rev. 1243, 21630 words, ARTICLE: Capitalism, Liberalism, and the Right to Privacy, Ofer Raban\*

683. Copyright (c) 2013 The University of Tulsa Tulsa Law Review, Summer, 2013, Tulsa Law Review, 49 Tulsa L. Rev. 183, 21252 words, NOTE & COMMENT: THE SHRINKING WINDOW OF PRIVACY: THE DECISION IN SKINNER AND HOW IT OPENS WIDER THE PRYING EYES OF THE GOVERNMENT, Micah J. Petersen

684. Copyright (c) 2014 Regents of the University of California UC Davis Law Review, June, 2014, UC Davis Law Review, 47 U.C. Davis L. Rev. 1539, 27095 words, ARTICLE: Watching Me: The War on Crime, Privacy, and the State, Kimberly D. Bailey\*

685. Copyright (c) 2013 Regents of the University of California UC Davis Law Review, April, 2013, UC Davis Law Review, 46 U.C. Davis L. Rev. 1175, 24604 words, ARTICLE: Institutional Competence to Balance Privacy and Competing Values: The Forgotten Third Prong of HIPAA Preemption Analysis, Barbara J. Evans\*

686. Copyright (c) 2011 Regents of the University of California UC Davis Law Review, December, 2011, UC Davis Law Review, 45 U.C. Davis L. Rev. 531, 30614 words, ARTICLE: Sex, Privacy, and Public Health in a Casual Encounters Culture, Mary D. Fan\*

687. Copyright (c) 2010 Regents of the University of California UC Davis Law Review, February, 2010, UC DAVIS LAW REVIEW, 43 U.C. Davis L. Rev. 715, 15340 words, SYMPOSIUM: THE HONORABLE JOHN PAUL STEVENS: LIBERTY: THE S0-CALLED RIGHT TO PRIVACY, Jamal Greene\*

688. Copyright (c) 2010 The Regents of the University of California U.C. Davis Journal of International Law & Policy, Spring, 2010, U.C. Davis Journal of International Law & Policy, 16 U.C. Davis J. Int'l L. & Pol'y 383, 26256 words, ARTICLE: The Twilight Zone of Privacy for Passengers on International Flights Between the EU & USA, Alenka Kuhelj\*

689. Copyright (c) 2010 The Regents of the University of California UCLA Law Review, August, 2010, UCLA Law Review, 57 UCLA L. Rev. 1701, 36013 words, ARTICLE: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, Paul Ohm\*

690. Copyright (c) 2012 Utah Law Review Society Utah Law Review, 2012, Utah Law Review, 2012 Utah L. Rev. 2023, 22243 words, ARTICLE: Juror Privacy in the Sixth Amendment Balance, Melanie D. Wilson\*

691. Copyright (c) 2010 Utah Law Review Society Utah Law Review, 2010, Utah Law Review, 2010 Utah L. Rev. 1277, 18627 words, Article: A Ticking Time Bomb? University Data Privacy Policies and Attorney-Client Confidentiality in Law School Settings, Gregory C. Sisk\* & Nicholas Halbur\*\*

692. Copyright (c) 2010 Valparaiso University Law Review Valparaiso University Law Review, Winter, 2010, Valparaiso University Law Review, 44 Val. U.L. Rev. 391, 15940 words, ARTICLE: TEACHING PRIVACY IN THE AGE OF OCTOMOM: ENHANCING CASE/SOCRATIC METHOD WITH STRUCTURED CLASS DISCUSSION, Constance Anastopoulo and Thomas P. Gressette, Jr. \*

693. Copyright (c) 2013 Vanderbilt Journal of Entertainment and Technology Law Vanderbilt Journal of Entertainment and Technology Law, Fall, 2013, Vanderbilt Journal of Entertainment and Technology Law, 16 Vand. J. Ent. & Tech. L. 103, 15195 words, ARTICLE: Sexual Privacy in the Internet Age: How Substantive Due Process Protects Online Obscenity, Jennifer M. Kinsley\*

694. Copyright (c) 2014 Vanderbilt Journal of Entertainment and Technology Law Vanderbilt Journal of Entertainment and Technology Law, Summer, 2014, Vanderbilt Journal of Entertainment and Technology Law, 16 Vand. J. Ent. & Tech. L. 701, 22974 words, ARTICLE: Fool's Gold: An Illustrated Critique of Differential Privacy, Jane Bambauer,\* Krishnamurty Muralidhar,\*\* and Rathindra Sarathy\*\*\*

695. Copyright (c) 2013 Vanderbilt Journal of Entertainment and Technology Law Vanderbilt Journal of Entertainment and Technology Law, Spring, 2013, Vanderbilt Journal of Entertainment and Technology Law \*, 15 Vand. J. Ent. & Tech. L. 713, 21572 words, NOTE: Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection, Timothy J. Van Hal\*

696. Copyright (c) 2012 Vanderbilt Journal of Entertainment and Technology Law Vanderbilt Journal of Entertainment and Technology Law, Spring, 2012, Vanderbilt Journal of Entertainment and Technology Law \*, 14 Vand. J. Ent. & Tech. L. 603, 24089 words, Article: Virtual Blinds: Finding Online Privacy in Offline Precedents, Allyson W. Haynes\*

697. Copyright (c) 2010 Vanderbilt Journal of Entertainment and Technology Law Vanderbilt Journal of Entertainment and Technology Law, Fall, 2010, Vanderbilt Journal of Entertainment and Technology Law, 13 Vand. J. Ent. & Tech. L. 217, 20932 words, NOTE: Google Books: Page by Page, Click by Click, Users Are Reading Away Privacy Rights, Kathleen E. Kubis\*

698. Copyright (c) 2011 Vanderbilt Journal of Entertainment and Technology Law Vanderbilt Journal of Entertainment and Technology Law, Winter, 2011, Vanderbilt Journal of Entertainment and Technology Law, 13 Vand. J. Ent. & Tech. L. 323, 17092 words, ARTICLE: Putting the Shock Value in First Amendment Jurisprudence: When Freedom for the Citizen-Journalist Watchdog Trumps the Right of Informational Privacy on the Internet, By Clay Calvert\* and Mirelis Torres\*\*

699. Copyright (c) 2011 Vanderbilt Journal of Entertainment and Technology Law Vanderbilt Journal of Entertainment and Technology Law, Winter, 2011, Vanderbilt Journal of Entertainment and Technology Law, 13 Vand. J. Ent. & Tech. L. 441, 12499 words, NOTE: Electronic Health Records and Respect for Patient Privacy: A Prescription for Compatibility, Lauren Bair Jacques\*

700. Copyright (c) 2011 Vanderbilt Journal of Entertainment and Technology Law Vanderbilt Journal of Entertainment and Technology Law, Spring, 2011, Vanderbilt Journal of Entertainment and Technology Law, 13 Vand. J. Ent. & Tech. L. 617, 22018 words, NOTE: Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud, Ilana R. Kattan\*

701. Copyright (c) 2010 Vanderbilt Journal of Entertainment and Technology Law Vanderbilt Journal of Entertainment and Technology Law, Spring, 2010, Vanderbilt Journal of Entertainment and Technology Law, 12 Vand. J. Ent. & Tech. L. 581, 13131 words, NOTE: The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege, Nathan K. McGregor\*

702. Copyright (c) 2011 Vanderbilt Law Review, Vanderbilt University Law School Vanderbilt Law Review, May, 2011, Vanderbilt Law Review, 64 Vand. L. Rev. 1347, 22151 words, NOTE: Text Offenders: Privacy, Text Messages, and the Failure of the Title III Minimization Requirement, Seth M. Hyatt\*

703. Copyright (c) 2010 Vanderbilt Law Review, Vanderbilt University Law School Vanderbilt Law Review, May, 2010, Vanderbilt Law Review, 63 Vand. L. Rev. 1131, 14914 words, NOTE: Street Shootings: Covert Photography and Public Privacy, Nancy Danforth Zeronda\*

704. Copyright (c) 2010 Vanderbilt Law Review, Vanderbilt University Law School Vanderbilt Law Review, October, 2010, Vanderbilt Law Review, 63 Vand. L. Rev. 1295, 30815 words, ARTICLE: The Puzzle of Brandeis, Privacy, and Speech, Neil M. Richards\*

705. Copyright (c) 2011 Vermont Law School Vermont Law Review, Winter, 2011, Vermont Law Review, 36 Vt. L. Rev. 471, 16020 words, NOTE: AUTOMATIC CONSUMER PRIVACY RIGHTS EMBEDDED IN SMART GRID TECHNOLOGY STANDARDS BY THE FEDERAL GOVERNMENT, -Lauren Reilly\*

706. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 809, 2535 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTER SORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW & UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: FOREWORD, John M. Greabe\*

707. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 817, 3082 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTER SORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW & UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: TRANSCRIPT: SORRELL V. IMS HEALTH AND THE SHIFT TO REGULATION BY PAYMENT, Ted Ruger\*+

708. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 823, 2197 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTER SORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW & UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: TRANSCRIPT: THE CASE FOR NATIONAL POLITICAL (RATHER THAN STATE OR JUDICIAL) REGULATION OF HEALTH CARE, Abigail R. Moncrieff\*+

709. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 829, 2782 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTER SORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW & UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: TRANSCRIPT: SORRELL V. IMS HEALTH-ANY IMPACT ON PATIENT PRIVACY?, John Verdi\*+

710. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 835, 1734 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTER SORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW & UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: TRANSCRIPT: COMMENTS ON THE ORIGINAL LEGISLATION AND VERMONT HEALTH REFORM, Steve Maier\*+

711. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 839, 1999 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTER SORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW & UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: REMARKS: A LEGISLATOR'S LAMENT: WHEN WILL WE TAKE BACK OUR ELECTRONIC IDENTITIES?, Sharon Anglin Treat\*+

712. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 845, 5854 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTERSORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW &UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: UNCENSORED DISCOURSE IS NOT JUST FOR POLITICS, Calvin Massey\*+

713. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 855, 14118 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTER SORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW & UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: SORRELL V. IMS HEALTH: DETAILS, DETAILING, AND THE DEATH OF PRIVACY, Ashutosh Bhagwat\*+

714. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 881, 10287 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTER SORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW & UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: THE DOG THAT DID BARK: FIRST AMENDMENT PROTECTION OF DATA MINING, Thomas R. Julin, Jamie Z. Isani and Patricia Acosta\*

715. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 903, 13257 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTER SORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW & UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: Sorrell v. IMS Health and the End of the Constitutional Double Standard, Ernest A. Young\*

716. Copyright (c) 2012 Vermont Law School Vermont Law Review, Summer, 2012, Vermont Law Review, 36 Vt. L. Rev. 931, 33008 words, CONSTITUTIONAL CONSTRAINTS ON STATE HEALTH CARE & PRIVACY REGULATION AFTER SORRELL V. IMS HEALTH: SYMPOSIUM-OCTOBER 14, 2011: VERMONT LAW REVIEW & UNIVERSITY OF NEW HAMPSHIRE LAW REVIEW: SOMEBODY'S WATCHING ME: PROTECTING PATIENT PRIVACY IN PRESCRIPTION HEALTH INFORMATION, Christopher R. Smith\*+

717. Copyright (c) 2011 Virginia Journal of Law and Technology Virginia Journal of Law and Technology, Spring, 2011, Virginia Journal of Law and Technology, 16 Va. J.L. & Tech. 189, 18884 words, ARTICLE: Constitutional Protection of "Sexting" in the Wake of Lawrence: The Rights of Parents and Privacy, CLAUDIO J. PAVIA+

718. Copyright (c) 2011 Virginia Journal of Law and Technology Virginia Journal of Law and Technology, Summer, 2011, Virginia Journal of Law and Technology, 16 Va. J.L. & Tech. 253, 25726 words, ARTICLE: What the Cops Can't Do, Internet Service Providers Can: Preserving Privacy in Email Contents, STEVEN R. MORRISON +

719. Copyright (c) 2011 Virginia Journal of Law and Technology Virginia Journal of Law and Technology, Winter, 2011, Virginia Journal of Law and Technology, 16 Va. J.L. & Tech. 499, 26283 words, ARTICLE: Towards a Brighter Fourth Amendment: Privacy and Technological Change, JOSHUA S. LEVY +

720. Copyright (c) 2012 University of Virginia School of Law Virginia Sports & Entertainment Law Journal, Spring, 2012, Virginia Sports & Entertainment Law Journal, 11 Va. Sports & Ent. L.J. 460, 25526 words, Article: Athlete Privacy Rights and Endorsement Contracts: An Analysis of U.S., U.K., and Australian Law, Paul A Czarnota\*

721. Copyright (c) 2014 Wake Forest Law Review Association, Inc. Wake Forest Law Review, Summer, 2014, Wake Forest Law Review, 49 Wake Forest L. Rev. 261, 22210 words, ARTICLE: ALAN WESTIN'S PRIVACY HOMO ECONOMICUS, Chris Jay Hoofnagle\* and Jennifer M. Urban\*\*

722. Copyright (c) 2014 Wake Forest Law Review Association, Inc. Wake Forest Law Review, Summer, 2014, Wake Forest Law Review, 49 Wake Forest L. Rev. 433, 22881 words, ARTICLE: THE RIGHT TO ERASURE: PRIVACY, DATA BROKERS, AND THE INDEFINITE RETENTION OF DATA, Alexander Tsesis\*

723. Copyright (c) 2010 Wake Forest Law Review Association, Inc. Wake Forest Law Review, Fall, 2010, Wake Forest Law Review, 45 Wake Forest L. Rev. 689, 20593 words, ARTICLE: PRIVATE ORDERING: A CONTRACTUAL APPROACH TO ONLINE INTERPERSONAL PRIVACY, Patricia Sanchez Abril\*

724. Copyright (c) 2014 Washburn Law Journal Washburn Law Journal, Spring, 2014, Washburn Law Journal, 53 Washburn L.J. 207, 33957 words, ARTICLE: The Right to Be Let Alone: The Kansas Right of Privacy, J. Lyn Entrikin\*

725. Copyright (c) 2010 Washington and Lee University Washington and Lee Journal of Civil Rights and Social Justice, Fall, 2010, Washington and Lee Journal of Civil Rights and Social Justice, 17 Wash. & Lee J. Civil Rts. & Soc. Just. 141, 13710 words, ARTICLE: A Failure to Communicate: Did Privacy Laws Contribute to the Virginia Tech Tragedy?, Richard Brusca and Colin Ram \*

726. Copyright (c) 2013 Washington & Lee University School of Law Washington & Lee Law Review, Winter, 2013, Washington & Lee Law Review, 70 Wash & Lee L. Rev. 341, 45977 words, Article: Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency, Jay P. Kesan\*, Carol M. Hayes\*\* and Masooda N. Bashir\*\*\*

727. Copyright (c) 2010 Washington & Lee University School of Law Washington & Lee Law Review, Spring, 2010, Washington & Lee Law Review, 67 Wash & Lee L. Rev. 589, 30136 words, ARTICLE: The Story of Us: Resolving the Face-Off Between Autobiographical Speech and Information Privacy, Sonja R. West \*

728. Copyright (c) 2011 Wayne State University The Wayne Law Review, Spring, 2011, Wayne Law Review, 57 Wayne L. Rev. 1, 4877 words, ARTICLE: NAKED SCANNERS, GPS TRACKING, AND PRIVATE CITIZENS: TECHNOLOGY'S ROLE IN BALANCING SECURITY AND PRIVACY, JEFFREY ROSEN +

729. Copyright (c) 2011 Wayne State University The Wayne Law Review, Spring, 2011, Wayne Law Review, 57 Wayne L. Rev. 271, 1890 words, ARTICLE: THE DEMISE OF PRIVACY: MICHIGAN CASES POST 9/11, KARY L. MOSS +

730. Copyright (c) 2011 West Virginia Law Review West Virginia Law Review, Fall 2011, West Virginia Law Review, 114 W. Va. L. Rev. 277, 19180 words, STUDENT WORK: AN ILLUSORY EXPECTATION OF PRIVACY: THE ECPA IS INSUFFICIENT TO PROVIDE MEANINGFUL PROTECTION FOR ADVANCED COMMUNICATION TOOLS, Sara E. Brown \*

731. Copyright (c) 2012 West Virginia Law Review West Virginia Law Review, Winter, 2012, West Virginia Law Review, 114 W. Va. L. Rev. 461, 31157 words, ARTICLE: TOWARD A COHESIVE INTERPRETATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT FOR THE ELECTRONIC MONITORING OF EMPLOYEES, Ariana R. Levinson \*

732. Copyright (c) 2011 Western New England Law Review Association, Inc. Western New England Law Review, 2011, Western New England Law Review, 33 W. New Eng. L. Rev. 211, 18352 words, NOTE: SUBSTANTIVE DUE PROCESS/PRIVACY--Stay Calm, Don't Get Hysterical: A User's Guide to Arguing the Unconstitutionality of Anti-Vibrator Statutes, Julie McKenna\*

733. Copyright (c) 2012 by the Western State University Law Review Association, Inc. Western State University Law Review, Spring, 2012, Western State University Law Review, 39 W. St. U. L. Rev. 187, 9688 words, ARTICLE: Place Doesn't Apply To My Place; The California Home Is Sui Generis Because Medical Marijuana Is Not Contraband and Indiscriminate Residential Dog Sniffs Invade a Patient's Legitimate Expectation of Privacy, Jared Willis\*

734. Copyright (c) 2013 Widener University School of Law Widener Law Journal, 2013, Widener Law Journal, 22 Widener L.J. 435, 8207 words, ANNUAL SURVEY OF PENNSYLVANIA ADMINISTRATIVE LAW: RIGHT-TO-KNOW-LAW: AGENCY'S EMAIL PRIVACY TRUMPS DISCLOSURE OF PUBLIC RECORDS UNDER THE PENNSYLVANIA RIGHT-TO-KNOW LAW: A SURVEY ANALYZING THE HOLDING OF EASTON AREA SCHOOL DISTRICT V. BAXTER AND THE COURT'S BATTLE WITH IDENTIFYING EMAILS AS PUBLIC RECORDS, Jolee Van Horn \*

735. Copyright (c) 2010 Widener University School of Law Widener Law Journal, 2010, Widener Law Journal, 19 Widener L.J. 577, 6883 words, ANNUAL SURVEY OF PENNSYLVANIA ADMINISTRATIVE LAW: OPEN RECORDS LAW: STRIKING A BALANCE BETWEEN PUBLIC INTEREST OF TRANSPARENCY OF GOVERNMENT AND THE PRIVACY OF PERSONAL IDENTIFICATION AND SECURITY INFORMATION: AN EXAMINATION OF TRIBUNE-REVIEW PUBLISHING CO. V BODACK, Lindsay M. Schoeneberger

736. Copyright (c) 2010 Widener University School of Law Widener Law Journal, 2010, Widener Law Journal, 19 Widener L.J. 793, 14502 words, SYMPOSIUM: INTERNET EXPRESSION IN THE 21ST CENTURY: WHERE TECHNOLOGY & LAW COLLIDE: PRIVACY AS PRODUCT SAFETY, James Grimmelmann\*

737. Copyright (c) 2010 Widener University School of Law Widener Law Journal, 2010, Widener Law Journal, 19 Widener L.J. 873, 8546 words, SYMPOSIUM: INTERNET EXPRESSION IN THE 21ST CENTURY: WHERE TECHNOLOGY & LAW COLLIDE: PRIVACY IS THE PROBLEM, Raymond Shih Ray Ku\*

738. Copyright (c) 2010 Widener University School of Law Widener Law Journal, 2010, Widener Law Journal, 19 Widener L.J. 893, 17037 words, SYMPOSIUM: INTERNET EXPRESSION IN THE 21ST CENTURY: WHERE TECHNOLOGY & LAW COLLIDE: PRIVACY PARADOX 2.0, H. Brian Holland\*

739. Copyright (c) 2013 Widener University School of Law Widener Law Review, 2013, Widener Law Review, 19 Widener L. Rev. 345, 20170 words, ARTICLE: THE INVASION OF PRIVACY ACT: THE DISCLOSURE OF MY INFORMATION IN YOUR GOVERNMENT FILE, Lieutenant Colonel Evan M. Stone\*

740. Copyright (c) 2012 Willamette Law Review Willamette Law Review, Winter, 2012, Willamette Law Review, 49 Willamette L. Rev. 251, 8704 words, ARTICLE: PRIVACY IN THE WORKPLACE: ARE COLLECTIVE BARGAINING AGREEMENTS A PLACE TO START FORMULATING MORE UNIFORM STANDARDS?, Karin Mika\*

741. Copyright (c) 2013 Publications Council of the College of William and Mary William & Mary Bill of Rights Journal, December, 2013, William & Mary Bill of Rights Journal, 22 Wm. & Mary Bill of Rts. J. 571, 17456 words, SYMPOSIUM: PROFESSOR CHARLES H. KOCH, JR. MEMORIAL SYMPOSIUM ON ADMINISTRATIVE LAW: ADMINISTRATIVE SEARCHES, TECHNOLOGY AND PERSONAL PRIVACY, Russell L. Weaver\*

742. Copyright (c) 2011 Publications Council of the College of William and Mary William & Mary Bill of Rights Journal, May, 2011, William and Mary Bill of Rights Journal, 19 Wm. & Mary Bill of Rts. J. 857, 365 words, SYMPOSIUM: PRIVACY, DEMOCRACY, AND ELECTIONS: IN MEMORIAM: JOSEPH PAUL DOYLE, Justin M. Marchesi\*

743. Copyright (c) 2011 Publications Council of the College of William and Mary William & Mary Bill of Rights Journal, May, 2011, William and Mary Bill of Rights Journal, 19 Wm. & Mary Bill of Rts. J. 859, 13384 words, SYMPOSIUM: PRIVACY, DEMOCRACY, AND ELECTIONS: MRS. MCINTYRE'S PERSONA: BRINGING PRIVACY THEORY TO ELECTION LAW, William McGeveran\*

744. Copyright (c) 2011 Publications Council of the College of William and Mary William & Mary Bill of Rights Journal, May, 2011, William and Mary Bill of Rights Journal, 19 Wm. & Mary Bill of Rts. J. 885, 10765 words, SYMPOSIUM: PRIVACY, DEMOCRACY, AND ELECTIONS: INTERNET VOTING, SECURITY, AND PRIVACY, Jeremy Epstein\*

745. Copyright (c) 2011 Publications Council of the College of William and Mary William & Mary Bill of Rights Journal, May, 2011, William and Mary Bill of Rights Journal, 19 Wm. & Mary Bill of Rts. J. 907, 10689 words, SYMPOSIUM: PRIVACY, DEMOCRACY, AND ELECTIONS: ONLINE BEHAVIORAL ADVERTISING AND DECEPTIVE CAMPAIGN TACTICS: POLICY ISSUES, Nichole Rustin-Paschal\*

746. Copyright (c) 2011 Publications Council of the College of William and Mary William & Mary Bill of Rights Journal, May, 2011, William and Mary Bill of Rights Journal, 19 Wm. & Mary Bill of Rts. J. 927, 16827 words, SYMPOSIUM: PRIVACY, DEMOCRACY, AND ELECTIONS: ANONYMITY AND DEMOCRATIC CITIZENSHIP, James A. Gardner\*

747. Copyright (c) 2011 Publications Council of the College of William and Mary William & Mary Bill of Rights Journal, May, 2011, William and Mary Bill of Rights Journal, 19 Wm. & Mary Bill of Rts. J. 959, 14515 words, SYMPOSIUM: PRIVACY, DEMOCRACY, AND ELECTIONS: CAMPAIGN DISCLOSURE, PRIVACY AND TRANSPARENCY, Deborah G. Johnson, Priscilla M. Regan, and Kent Wayland\*

748. Copyright (c) 2011 Publications Council of the College of William and Mary William & Mary Bill of Rights Journal, May, 2011, William and Mary Bill of Rights Journal, 19 Wm. & Mary Bill of Rts. J. 983, 22298 words, SYMPOSIUM: PRIVACY, DEMOCRACY, AND ELECTIONS: TWO CHALLENGES FOR CAMPAIGN FINANCE DISCLOSURE AFTER CITIZENS UNITED AND DOE V. REED, Richard Briffault\*

749. Copyright (c) 2010 The College of William and Mary William and Mary Journal of Women and the Law, Winter, 2010, WILLIAM & MARY JOURNAL OF WOMEN AND THE LAW, 16 Wm. & Mary J. of Women & L. 237, 25601 words, 2009 SYMPOSIUM: FROM THE COURTROOM TO THE MOTHER'S WOMB: PROTECTING WOMEN'S PRIVACY IN THE MOST IMPORTANT PLACES: ARTICLE: PRIVACY AND DOMESTIC VIOLENCE IN COURT, Rebecca Hulse\*

750. Copyright (c) 2010 The College of William and Mary William and Mary Journal of Women and the Law, Winter, 2010, WILLIAM & MARY JOURNAL OF WOMEN AND THE LAW, 16 Wm. & Mary J. of Women & L. 291, 18451 words, 2009 SYMPOSIUM: FROM THE COURTROOM TO THE MOTHER'S WOMB: PROTECTING WOMEN'S PRIVACY IN THE MOST IMPORTANT PLACES: ARTICLE: ABORTION, THE UNDUE BURDEN STANDARD, AND THE EVISCERATION OF WOMEN'S PRIVACY, Caitlin E. Borgmann\*

751. Copyright (c) 2010 The College of William and Mary William and Mary Journal of Women and the Law, Winter, 2010, WILLIAM & MARY JOURNAL OF WOMEN AND THE LAW, 16 Wm. & Mary J. of Women & L. 327, 21969 words, 2009 SYMPOSIUM: FROM THE COURTROOM TO THE MOTHER'S WOMB: PROTECTING WOMEN'S PRIVACY IN THE MOST IMPORTANT PLACES: ARTICLE: TAXATION, PREGNANCY, AND PRIVACY, Bridget J. Crawford\*

752. Copyright (c) 2010 The College of William and Mary William and Mary Journal of Women and the Law, Winter, 2010, WILLIAM & MARY JOURNAL OF WOMEN AND THE LAW, 16 Wm. & Mary J. of Women & L. 369, 11238 words, 2009 SYMPOSIUM: FROM THE COURTROOM TO THE MOTHER'S WOMB: PROTECTING WOMEN'S PRIVACY IN THE MOST IMPORTANT PLACES: ARTICLE: MEDICAL CONSCIENCE AND THE POLICING OF PARENTHOOD, Richard F. Storrow\*

753. Copyright (c) 2010 The College of William and Mary William and Mary Journal of Women and the Law, Winter, 2010, WILLIAM & MARY JOURNAL OF WOMEN AND THE LAW, 16 Wm. & Mary J. of Women & L. 395, 13148 words, 2009 SYMPOSIUM: FROM THE COURTROOM TO THE MOTHER'S WOMB: PROTECTING WOMEN'S PRIVACY IN THE MOST IMPORTANT PLACES: NOTE: THE GENDER GAP: A PERSISTENT PROBLEM THAT CONGRESS HAS YET TO ADDRESS, Leeron Avnery\*

754. Copyright (c) 2010 The College of William and Mary William and Mary Journal of Women and the Law, Winter, 2010, WILLIAM & MARY JOURNAL OF WOMEN AND THE LAW, 16 Wm. & Mary J. of Women & L. 423, 13761 words, 2009 SYMPOSIUM: FROM THE COURTROOM TO THE MOTHER'S WOMB: PROTECTING WOMEN'S PRIVACY IN THE MOST IMPORTANT PLACES: NOTE: KNOW YOUR LIMIT: HOW LEGISLATURES HAVE GONE OVERBOARD WITH PER SE DRUNK DRIVING LAWS AND HOW MEN PAY THE PRICE, Andrew Gore\*

755. Copyright (c) 2013 William & Mary Law Review William & Mary Law Review, April, 2013, William & Mary Law Review, 54 Wm. & Mary L. Rev. 1693, 8785 words, ARTICLE: PRIVACY AND CONSENT OVER TIME: THE ROLE OF AGREEMENT IN FOURTH AMENDMENT ANALYSIS, Christine Jolls\*

756. Copyright (c) 2010 William & Mary Law Review William & Mary Law Review, May, 2010, William and Mary Law Review, 51 Wm. & Mary L. Rev. 2243, 11146 words, ARTICLE: PAGING DR. GOOGLE: PERSONAL HEALTH RECORDS AND PATIENT PRIVACY, Colin P. McCarthy\*

757. Copyright (c) 2014 William Mitchell College of Law William Mitchell Law Review, 2014, William Mitchell Law Review, 40 Wm. Mitchell L. Rev. 849, 16557 words, ARTICLE: THE COSTS OF LOST PRIVACY: CONSUMER HARM AND RISING ECONOMIC INEQUALITY IN THE AGE OF GOOGLE, Nathan Newman+

758. Copyright (c) 2011 William Mitchell College of Law William Mitchell Law Review, 2011, William Mitchell Law Review, 38 Wm. Mitchell L. Rev. 290, 16133 words, CONTEMPORARY ISSUES IN CYBERLAW: MARKETING THROUGH SOCIAL NETWORKS: BUSINESS CONSIDERATIONS - FROM BRAND TO PRIVACY, Katheryn A. Andresen+

759. Copyright (c) 2011 William Mitchell College of Law William Mitchell Law Review, 2011, William Mitchell Law Review, 37 Wm. Mitchell L. Rev. 1671, 26706 words, ELECTRONIC COMMERCE LAW: PUTTING THE GENIE BACK IN THE BOTTLE: LEVERAGING PRIVATE ENFORCEMENT TO IMPROVE INTERNET PRIVACY, Jonathan D. Frieden, Esq.+, Charity M. Price, Esq.++, and Leigh M. Murray, Esq.+++

760. Copyright (c) 2011 William Mitchell College of Law William Mitchell Law Review, 2011, William Mitchell Law Review, 37 Wm. Mitchell L. Rev. 1727, 6427 words, ELECTRONIC COMMERCE LAW: THE FTC'S PROPOSED FRAMEWORK FOR PRIVACY PROTECTION ONLINE: A MOVE TOWARD SUBSTANTIVE CONTROLS OR JUST MORE NOTICE AND CHOICE?, James P. Nehf+

761. Copyright (c) 2011 Case Western Reserve University School of Law Canada - United States Law Journal, 2011, Canada - United States Law Journal, 36 Can.-U.S. L.J. 108, 5658 words, PROCEEDINGS OF THE CANADA-UNITED STATES LAW INSTITUTE HENRY T. KING, JR. ANNUAL CONFERENCE ON THE CANADA-UNITED STATES REGULATORY REGIME: REVIEW, REFORM, RECOVERY: CLEVELAND, OHIO: APRIL 8-10, 2010: ACHIEVING CANADA-UNITED STATES ECONOMIC COMPETITIVENESS THROUGH REGULATORY CONVERGENCE -- A COMMON CAUSE AGENDA: DIVERGENCE AND CONVERGENCE OF DATA PRIVACY RULES -- MYTH AND REALITY, By Paul A. Meyer n191

762. Copyright (c) 2014 Wisconsin Law Review Wisconsin Law Review, 2014, Wisconsin Law Review, 2014 Wis. L. Rev. 165, 14759 words, COMMENT: DISARMING KNOWLEDGE OR REVEALING THE CONCEALED: BALANCING DEMOCRATIC ACCOUNTABILITY AND PERSONAL PRIVACY FOR WISCONSIN'S CONCEALED CARRY PERMIT REGISTRY, Andrew W. Lang\*

763. Copyright (c) 2013 Wisconsin Law Review Wisconsin Law Review, 2013, Wisconsin Law Review, 2013 Wis. L. Rev. 649, 9306 words, SYMPOSIUM ISSUE: 30 YEARS OF COMPARATIVE INSTITUTIONAL ANALYSIS: A CELEBRATION OF NEIL KOMESAR: FINDING THE BEST OF THE IMPERFECT ALTERNATIVES FOR PRIVACY, HEALTH IT, AND CYBERSECURITY, Peter Swire\*

764. Copyright (c) 2010 Women's Rights Law Reporter--Rutgers, The State University of New Jersey Women's Rights Law Reporter, Summer, 2010, Women's Rights Law Reporter, 31 Women's Rights L. Rep. 447, 22617 words, ARTICLE: PERSONAL AUTONOMY: TOWARDS A NEW TAXONOMY FOR PRIVACY LAW, Yvonne F. Lindgren\*

765. Copyright (c) 2013 Yale Journal of Law & Technology Yale Journal of Law & Technology, 2013, Yale Journal of Law & Technology, 16 Yale J. L. & Tech. 1, 10274 words, ARTICLE: CONFIDENTIALITY AND THE PROBLEM OF THIRD PARTIES: PROTECTING READER PRIVACY IN THE AGE OF INTERMEDIARIES, BJ Ard \*

766. Copyright (c) 2013 Yale Journal of Law & Technology Yale Journal of Law & Technology, 2013 - 2014, Yale Journal of Law & Technology, 16 Yale J. L. & Tech. 59, 10643 words, ARTICLE: A THEORY OF CREEPY: TECHNOLOGY, PRIVACY AND SHIFTING SOCIAL NORMS, Omer Tene and Jules Polonetsky \*

767. Copyright (c) 2012 Yale Journal of Law & Technology Yale Journal of Law & Technology, Winter, 2012-2013, Yale Journal of Law & Technology, 15 Yale J. L. & Tech. 24, 10560 words, ARTICLE: REVERSE ENGINEERING INFORMATIONAL PRIVACY LAW, Michael Birnhack \*

768. Copyright (c) 2012 Yale Journal of Law & Technology Yale Journal of Law & Technology, Winter, 2012-2013, Yale Journal of Law & Technology, 15 Yale J. L. & Tech. 139, 10654 words, ARTICLE: MOVING FROM NIXON TO NASA: PRIVACY'S SECOND STRAND--A RIGHT TO INFORMATIONAL PRIVACY, Christina P. Moniodis \*

769. Copyright (c) 2013 The Yale Law Journal Company, Inc. The Yale Law Journal, November, 2013, Yale Law Journal, 123 Yale L.J. 513, 6217 words, COMMENT: The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy, JACOB M. VICTOR\*

770. Copyright (c) 2010 The Yale Law Journal Company, Inc. The Yale Law Journal, November, 2010, Yale Law Journal, 120 Yale L.J. 379, 8061 words, COMMENT: Privacy, Personhood, and the Courts: FOIA Exemption 7(C) in Context, SCOTT A. HARTMAN

771. Copyright (c) 2014 Boston Bar Association Boston Bar Journal, Spring, 2014, 58 B.B.J. 27, 1755 words, LEGAL ANALYSIS: ANY CALLS, TEXTS, OR PHOTOS MAY BE USED AGAINST YOU: WARRANTLESS CELL PHONE SEARCHES AND PERSONAL PRIVACY, by Gerard T. Leone, Linn Foster Freedman and Kathryn M. Silvia

772. Copyright (c) 2012 Boston Bar Association Boston Bar Journal, Fall, 2012, 56 B.B.J. 15, 1255 words, FEATURED ARTICLE: VANTAGE POINT: OH, THE PLACES YOU'VE BEEN! PRESERVING PRIVACY IN A CELLULAR AGE, By Sara E. Silva

773. Copyright (c) 2011 Boston Bar Association Boston Bar Journal, Summer, 2011, 55 B.B.J. 17, 2321 words, PRACTICE TIPS: SOCIAL NETWORKING, MOBILE DEVICES, AND THE CLOUD: THE NEWEST FRONTIERS OF PRIVACY LAW, By David J. Goldstone and Daniel B. Reagan

774. Copyright (c) 2010 Boston Bar Association Boston Bar Journal, Fall, 2010, 54 B.B.J. 29, 2685 words, ARTICLE: LEGAL ANALYSIS: TECHNOLOGY AND PRIVACY IN THE WORKPLACE: MONITORING EMPLOYEE COMMUNICATIONS AFTER THE SUPREME COURT'S QUON DECISION, By Ariel D. Cudkowicz, Kent D.B. Sinclair, and Erik W. Weibust

775. Copyright (c) 2010 by the Florida Bar The Florida Bar Journal, January, 2010, 84 Fla. Bar J. 56, 153 words, BOOK REVIEW: PRIVACY: THE LOST RIGHT

By Jon L. Mills, **Privacy:** The Lost Right (391 pages) is published by Oxford ...

776. Copyright © 2013 Hawaii State Bar Association Hawaii Bar Journal, October, 2013, 17 Hawaii B.J. 4, 9201 words, ARTICLE: PRIVACY EXPECTATIONS: A GLIMPSE INTO THE CONSTITUTIONAL RIGHT AGAINST UNREASONABLE SEARCHES AND SEIZURES, by Brandon H. Ito

777. Copyright (c) 2011 Houston Bar Association The Houston Lawyer, May/June, 2011, 48 Houston Lawyer 46, 584 words, DEPARTMENT: LEGAL TRENDS: THE U.S. SUPREME COURT RULES CORPORATIONS DO NOT HAVE "PERSONAL PRIVACY" UNDER THE FOIA, By Jill Yaziji

778. Copyright (c) 2011 Los Angeles County Bar Association Los Angeles Lawyer, September, 2011, 34 Los Angeles Lawyer 16, 3115 words, DEPARTMENT: PRACTICE TIPS: COURTS LIMIT THE PRIVACY RIGHTS OF PUBLIC AND PRIVATE EMPLOYEES, BY MATTHEW J. NORRIS

779. Copyright (c) 2010 Los Angeles County Bar Association Los Angeles Lawyer, June, 2010, 33 Los Angeles Lawyer 12, 3967 words, DEPARTMENT: PRACTICE TIPS: THE DIMINISHING POWER OF CALIFORNIA'S RIGHTS OF PRIVACY AND PUBLICITY, BY Zac Locke

780. Copyright (c) 2011 Louisiana Bar Journal Louisiana Bar Journal, October/November, 2011, 59 LA Bar Jnl. 180, 3893 words, FEATURE: CAMERA PHONES, PATIENT PRIVACY AND HIPAA: THE GROWING PROBLEM OF CAMERA PHONE ABUSE IN HEALTH-CARE FACILITIES, By Kimberly R. Silas

781. Copyright (c) 2010 Louisiana Bar Journal Louisiana Bar Journal, June/July, 2010, 58 LA Bar Jnl. 26, 1918 words, FEATURE: DID YOU TWITTER MY FACEBOOK(R) WALL? SOCIAL NETWORKING, PRIVACY AND EMPLOYMENT LAW ISSUES, By Michelle D. Craig

782. Copyright (c) 2014 by the State Bar of Michigan Michigan Bar Journal, May, 2014, 93 MI Bar Jnl. 24, 2194 words, PROBATE AND ESTATE PLANNING: BLENDED FAMILIES, PRIVACY, PITFALL AVOIDANCE, AND OTHER REASONS WHY ESTATE PLANNING LAWYERS REMAIN IMPORTANT, By Jeffrey D. Moss

783. Copyright (c) 2013 by the State Bar of Michigan Michigan Bar Journal, June, 2013, 92 MI Bar Jnl. 58, 1234 words, LAW PRACTICE SOLUTIONS: MANAGING THE SECURITY AND PRIVACY OF DATA IN A LAW OFFICE, By Dan Pinnington

784. Copyright (c) 2011 by the State Bar of Michigan Michigan Bar Journal, July, 2011, 90 MI Bar Jnl. 22, 3302 words, INFORMATION TECHNOLOGY LAW: INTERNET PRIVACY CONCERNS REIGNITED IN 2010, By Brian Balow and Tatiana Melnik

785. Copyright (c) 2013 State Bar of Montana The Montana Lawyer, October, 2013, 39 Montana Lawyer 5, 2251 words, FEATURE STORY: HEALTH CARE | PRIVACY: HIPAA, HITECH AND THE 2013 OMNIBUS CHANGES, By Darci Bentson

786. Copyright (c) 2011 State Bar of Montana The Montana Lawyer, October, 2011, 37 Montana Lawyer 23, 1082 words, COURT: NEW PRIVACY RULES TEMPORARILY SUSPENDED

787. Copyright (c) 2011 State Bar of Montana The Montana Lawyer, March, 2011, 36 Montana Lawyer 25, 630 words, FEATURE: LAW-OFFICE TECHNOLOGY: FAXING IN THE AGE OF PRIVACY, By Steve Adams

788. Copyright (c) 2011 State Bar of Montana The Montana Lawyer, February, 2011, 36 Montana Lawyer 21, 134 words, COURT: ONE MONTH LEFT ON COMMENTS ABOUT PRIVACY RULE CHANGES

789. Copyright (c) 2010 State Bar of Nevada Nevada Lawyer, November, 2010, 18 Nevada Lawyer 21, 1519 words, SPECIAL FEATURE: REQUESTING PROTECTED HEALTH INFORMATION FROM MILITARY MEDICAL TREATMENT FACILITIES: THE PRIVACY RULE MEETS THE PRIVACY ACT, By Major Charles G. Kels, USAF, Esq.

790. Copyright (c) 2011 by the Oregon State Bar The Oregon State Bar Bulletin, October, 2011, 72 Or. St. B. Bull. 19, 2285 words, FEATURE: THE RED HOT TRAIL: AS ELECTRONIC TRACKING TO ACCUMULATE EVIDENCE BECOMES MORE EXTENSIVE, MANY WORRY ABOUT THREAT TO PRIVACY RIGHTS, By Melody Finnemore

791. Copyright (c) 2011 Pennsylvania Bar Association Quarterly Pennsylvania Bar Association, October, 2011, 82 PA Bar Assn. Quarterly 139, 6934 words, ARTICLE: CURRENT DEVELOPMENTS IN PRIVACY AND SECURITY--IMPACT OF TECHNOLOGY, By Dorothy M. Bollinger, \* Delaware County AND Tristram R. Fall, III, \*\* Philadelphia County, Members of the Pennsylvania Bar

792. Copyright (c) 2014 by the Pennsylvania Bar Association The Pennsylvania Lawyer, July/August, 2014, 36 Pennsylvania Lawyer 36, 1797 words, FEATURE: PRIVACY VS. TECHNOLOGY, By Craig J. Staudenmaier

793. Copyright (c) 2013 by the Pennsylvania Bar Association The Pennsylvania Lawyer, September / October, 2013, 35 Pennsylvania Lawyer 24, 2533 words, ANNUAL TECH REPORT: WHAT WE'VE LOST, WHAT WE'VE GAINED: ARE WE LOSING PRIVACY BUT GAINING SOMETHING MORE IMPORTANT?, By David Narkiewicz

794. Copyright (c) 2010 by the Pennsylvania Bar Association The Pennsylvania Lawyer, September/October, 2010, 32 Pennsylvania Lawyer 18, 1744 words, PRO/CON: THE RIGHT TO PRIVACY AND PUBLIC EMPLOYMENT: HOME ADDRESSES OF PUBLIC EMPLOYEES: SUBJECT TO A RIGHT OF PRIVACY, By Andrea Bowman

795. Copyright (c) 2010 by the Pennsylvania Bar Association The Pennsylvania Lawyer, September/October, 2010, 32 Pennsylvania Lawyer 24, 1595 words, PRO/CON: THE RIGHT TO PRIVACY AND PUBLIC EMPLOYMENT: HOME ADDRESSES OF PUBLIC EMPLOYEES: KEEP THEM PUBLIC, By Craig J. Staudenmaier

796. Copyright (c) 2011 by the Rhode Island Bar Association Rhode Island Bar Journal, May/June, 2011, 59 RI Bar Jnl. 5, 3133 words, ARTICLE: NONE OF YOUR DAMN BUSINESS: INFORMATIONAL PRIVACY AFTER NELSON, Peter J. Comerford, Esq., Coia & Lepore, Ltd.

797. Copyright (c) 2010 South Carolina Bar South Carolina Lawyer, March, 2010, 21 S. Carolina Lawyer 16, 3669 words, ARTICLE: THE NEW HIPAA PRIVACY AND SECURITY RULES ARE HERE: WHAT DO YOUR CLIENTS NEED TO KNOW?, By Kelly M. Jolley and Kathleen G. Chewning

798. Copyright (c) 2011 by State Bar of Texas Texas Bar Journal, September, 2011, 74 Tex. B. J. 698, 1172 words, DEPARTMENT: TECHNOLOGY: KERRY, MCCAIN INTRODUCE BILL TO "CHECK IN" ON THE GROWING CONCERN OF ONLINE PRIVACY FOR END USERS, BY JOE THERIOT

799. Copyright (c) 2014 Tennessee Bar Association Tennessee Bar Journal, March, 2014, Tennessee Bar Journal, 50 Tenn. B.J. 16, 3863 words, COVER STORY: PRIVACY: WHAT LAWYERS MUST DO TO COMPLY WITH HIPAA: ACCOUNTABILITY EXPANDED FOR LAW FIRMS ACTING AS BUSINESS ASSOCIATES, By John V. Arnold

800. Copyright (c) 2013 Tennessee Bar Association Tennessee Bar Journal, July, 2013, Tennessee Bar Journal, 49 Tenn. B.J. 21, 2837 words, FEATURE STORY: WHEN A CHILD'S BEST INTERESTS ARE AT ISSUE: PRIVACY OF MENTAL HEALTH RECORDS IN DIVORCE AND CUSTODY PROCEEDINGS, By Siew-Ling Shea

801. Copyright (c) 2014 Utah State Bar Utah Bar Journal, May/June, 2014, 27 Utah Bar J. 20, 2689 words, ARTICLE: TO SNOOP OR NOT TO SNOOP? LEGAL CONSIDERATIONS UNDER UTAH'S INTERNET EMPLOYMENT PRIVACY ACT, by Christopher B. Snow

802. Copyright (c) 2013 Utah State Bar Utah Bar Journal, November / December, 2013, 26 Utah Bar J. 66, 1178 words, PARALEGAL DIVISION: PRIVACY & SECURITY: A QUICK LOOK INTO THE OMNIBUS FINAL RULE OF THE HIPAA & HITECH ACTS, by Heather J. Allen

803. Copyright (c) 2012 Utah State Bar Utah Bar Journal, January / February, 2012, 25 Utah Bar J. 26, 824 words, FOCUS ON ETHICS & CIVILITY: E-MAIL PRIVACY, by Keith A. Call

804. Copyright (c) 2011 National Association of Criminal Defense Lawyers, Inc. The Champion, December, 2011, 35 Champion 7, 1678 words, INSIDE NACDL: WILL 2012 BE A DEFINING YEAR FOR PRIVACY IN AMERICA? THE GPS CASE AND THE FUTURE OF THE DARKNESS ON THE EDGE OF TOWN, BY NORMAN L. REIMER

805. Copyright (c) 2010 National Association of Criminal Defense Lawyers, Inc. The Champion, August, 2010, 34 Champion 18, 10357 words, ARTICLE: THE PLAIN VIEW DOCTRINE AND COMPUTER SEARCHES: BALANCING LAW ENFORCEMENT'S INVESTIGATORY NEEDS WITH PRIVACY RIGHTS IN THE DIGITAL AGE, BY David H. Angeli, Christina Schuck, and Avalyn Taylor

806. Copyright (c) 2012 by Orange County Bar Association Orange County Lawyer, June, 2012, 54 Orange County Lawyer 28, 2002 words, FEATURE: CALIFORNIA-STYLE PRIVACY GOES NATIONAL, by CYRUS WADIA

807. Copyright © 2012 American Bar Association, ABA Journal, January, 2012, 98 A.B.A.J. 6, 342 words, Letters to the Editor, KEEPING AN EYE ON PRIVACY

808. Copyright © 2011 American Bar Association, ABA Journal, November, 2011, 97 A.B.A.J. 21, 1448 words, Supreme Court Report, Sky-High Spy: With GPS probing, the zone of privacy is getting even smaller, Mark Walsh

809. Copyright © 2011 American Bar Association, ABA Journal, October, 2011, 97 A.B.A.J. 28, 273 words, Business of Law, PRIVACY: OPEN SECRET: Cisco site shares privacy approach, Rachel M. Zahorsky, Edited by Reginald F. Davis reginald.davis@americanbar.org

810. Copyright © 2010 American Bar Association, ABA Journal, March, 2010, 96 A.B.A.J. 22, 1545 words, Supreme Court Report, Police De-text-ive: Is it a privacy violation to review messages on a work-issued pager?, Mark Hansen

811. Copyright (c) 2014 American Bar Association Administrative Law Review, Spring 2014, 66 ADMIN. L. REV. 463, 12103 words, COMMENT UNCHARTED TERRITORY: THE FAA AND THE REGULATION OF PRIVACY VIA RULEMAKING FOR DOMESTIC DRONES, MELISSA BARBEE\*

812. Copyright (c) 2013 American Bar Association The Business Lawyer, November, 2013, 69 Bus. Law. 217, 4553 words, SURVEY--CYBERSPACE LAW: COMMITTEE ON CYBERSPACE LAW, ABA BUSINESS LAW SECTION., Privacy in the Age of Big Data, John Pavolotsky \*

813. Copyright (c) 2013 American Bar Association The Business Lawyer, November, 2013, 69 Bus. Law. 227, 4796 words, SURVEY--CYBERSPACE LAW: COMMITTEE ON CYBERSPACE LAW, ABA BUSINESS LAW SECTION., Survey of Recent FTC Privacy Enforcement Actions and Developments, Fatima N. Khan \*

814. Copyright (c) 2013 American Bar Association The Business Lawyer, November, 2013, 69 Bus. Law. 237, 2881 words, SURVEY--CYBERSPACE LAW: COMMITTEE ON CYBERSPACE LAW, ABA BUSINESS LAW SECTION., Recent Developments in Mobile Privacy Law and Regulation, Robert V. Hale II \*

815. Copyright (c) 2013 American Bar Association The Business Lawyer, November, 2013, 69 Bus. Law. 245, 4948 words, SURVEY--CYBERSPACE LAW: COMMITTEE ON CYBERSPACE LAW, ABA BUSINESS LAW SECTION., Global Privacy and Data Security Developments--2013, Katherine Ritchey, Mauricio Paez, Veronica McGregor, and Maria Sendra \*

816. Copyright (c) 2012 American Bar Association The Business Lawyer, November, 2012, 68 Bus. Law. 197, 4119 words, SURVEY--CYBERSPACE LAW: COMMITTEE ON CYBERSPACE LAW, ABA SECTION OF BUSINESS LAW., Developments in the Law Concerning Geolocational Privacy, Theodore F. Claypoole and Richard C. Balough \*

817. Copyright (c) 2012 American Bar Association The Business Lawyer, November, 2012, 68 Bus. Law. 205, 4129 words, SURVEY--CYBERSPACE LAW: COMMITTEE ON CYBERSPACE LAW, ABA SECTION OF BUSINESS LAW., Survey of Recent European Union Privacy Developments, W. Gregory Voss \*

818. Copyright (c) 2012 American Bar Association The Business Lawyer, November, 2012, 68 Bus. Law. 215, 4066 words, SURVEY--CYBERSPACE LAW: COMMITTEE ON CYBERSPACE LAW, ABA SECTION OF BUSINESS LAW., The EU E-Privacy Directive and Consent to Cookies, Robert Bond \*

819. Copyright (c) 2012 American Bar Association The Business Lawyer, November, 2012, 68 Bus. Law. 225, 3234 words, SURVEY--CYBERSPACE LAW: COMMITTEE ON CYBERSPACE LAW, ABA SECTION OF BUSINESS LAW., Survey of Recent FTC Privacy Enforcement Actions and Developments, Fatima Nadine Khan \*

820. Copyright (c) 2012 American Bar Association Antitrust, Fall, 2012, 27 Antitrust ABA 81, PERSPECTIVES ON CHANGE DEVELOPMENTS IN CONSUMER PROTECTION: PRIVACY AS A FIELD OF LAW AND THE MOVE TO ENFORCEMENTS IN FEDERAL COURT, By Joan Z. Bernstein

821. Copyright (c) 2012 American Bar Association Antitrust, Summer, 2012, 26 Antitrust ABA 8, COVER STORY SO CLOSE, YET SO FAR APART: THE EU AND U.S. VISIONS OF A NEW PRIVACY FRAMEWORK, By Christopher Wolf and Winston Maxwell

822. Copyright (c) 2011 American Bar Association The Business Lawyer, November, 2011, 67 Bus. Law. 297, 3352 words, SURVEY--CYBERSPACE LAW; COMMITTEE ON CYBERSPACE LAW, ABA SECTION OF BUSINESS LAW, Survey of Recent FTC Privacy Developments and Enforcement, Fatima Khan \*

823. Copyright (c) 2011 American Bar Association Antitrust, Spring, 2011, 25 Antitrust ABA 43, COVER STORY: THE FTC'S NEW PRIVACY FRAMEWORK, BY Maureen K. Ohlhausen

824. Copyright (c) 2011 American Bar Association The Business Lawyer, February, 2011, 66 Bus. Law. 483, 6290 words, SURVEY--CONSUMER FINANCIAL SERVICES LAW: COMMITTEE ON CONSUMER FINANCIAL SERVICES, ABA SECTION OF BUSINESS LAW., 2010 Privacy and Data Security Developments, Patricia E.M. Covington and Meghan Musselman \*

825. Copyright (c) 2010 American Bar Association The Business Lawyer, February, 2010, 65 Bus. Law. 611, 5519 words, SURVEY--CONSUMER FINANCIAL SERVICES LAW: COMMITTEE ON CONSUMER FINANCIAL SERVICES, ABA SECTION OF BUSINESS LAW., Recent Privacy and Data Security Developments, Patricia E.M. Covington and Meghan S. Musselman \*

826. Copyright (c) 2012 American Bar Association GPSolo, November/December, 2012, 29 GPSolo 8, FEATURE WHAT ARE THE LIMITS OF EMPLOYEE PRIVACY?, By Diane Vaksdal Smith and Jacob Burg

827. Copyright (c) 2012 American Bar Association GPSolo, November/December, 2012, 29 GPSolo 8, FEATURES WHAT ARE THE LIMITS OF EMPLOYEE PRIVACY?, By Diane Vaksdal Smith and Jacob Burg

828. Copyright (c) 2012 American Bar Association GPSolo, November/December, 2012, 29 GPSolo 12, FEATURE TO SNOOP OR NOT TO SNOOP PRIVACY RIGHTS OF APPLICANTS AND POTENTIAL EMPLOYEES, By Edith L. Curry

829. Copyright (c) 2012 American Bar Association GPSolo, November/December, 2012, 29 GPSolo 12, FEATURES TO SNOOP OR NOT TO SNOOP: PRIVACY RIGHTS OF APPLICANTS AND POTENTIAL EMPLOYEES, By Edith L. Curry

830. Copyright (c) 2012 American Bar Association GPSolo, November/December, 2012, 29 GPSolo 30, FEATURE PRIVACY AND LEGAL OUTSOURCING, By William L. Pfeifer Jr.

831. Copyright (c) 2012 American Bar Association GPSolo, November/December, 2012, 29 GPSolo 30, FEATURES PRIVACY AND LEGAL OUTSOURCING, By William L. Pfeifer Jr.

832. Copyright (c) 2012 American Bar Association GPSolo, November/December, 2012, 29 GPSolo 48, FEATURE ADVISING CLIENTS ON INTERNET PRIVACY POLICIES, By Michelle Sherman

833. Copyright (c) 2012 American Bar Association GPSolo, November/December, 2012, 29 GPSolo 48, FEATURES ADVISING CLIENTS ON INTERNET PRIVACY POLICIES, By Michelle Sherman

834. Copyright (c) 2012 American Bar Association GPSolo, November/December, 2012, 29 GPSolo 66, COLUMN READY RESOURCES READY RESOURCES IN PRIVACY AND CONFIDENTIALITY

835. Copyright (c) 2012 American Bar Association GPSolo, November/December, 2012, 29 GPSolo 66, COLUMNS READY RESOURCES READY RESOURCES IN PRIVACY AND CONFIDENTIALITY

836. Copyright (c) 2011 American Bar Association GPSolo, June, 2011, 28 GPSolo 34, FEATURE PRIVACY IN AN INTERCONNECTED WORLD, By Andrew B. Serwin, M. Leeann Habte, and Jerry D. Brown

837. Copyright (c) 2011 American Bar Association Jurimetrics, Summer, 2011, 51 Jurimetrics J. 447, BOOK REVIEW PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE A QUEST FOR A THEORY OF PRIVACY: CONTEXT AND CONTROL, Michael D. Birnhack \*

838. Copyright (c) 2014 American Bar Association The ABA Journal of Labor and Employment Law, Winter, 2014, 29 ABA Journal Lab. & Emp. Law 229, NAVIGATING INTERNATIONAL DISCOVERY AND EUROPEAN DATA PRIVACY, Robert D. Kraus \* & Kristin M. Gallagher \*\*

839. Copyright (c) 2013 American Bar Association Criminal Justice, Summer, 2013, 28 Crim. Just. 36, DEPARTMENT TECHNOLOGY BORDERLINE PRIVACY: ELECTRONIC BORDER SEARCHES AFTER COTTERMAN, By Louisa K. Marion

840. Copyright (c) 2011 American Bar Association Litigation, Fall, 2011, 38 Litigation 17, COLUMN: IWITNESS THE CHALLENGE OF ELECTRONIC COMMUNICATIONS: PRIVILEGE, PRIVACY, AND OTHER MYTHS, JOHN M. BARKETT

841. Do Lawyers Violate the Driver's Privacy Protection Act When They Obtain Drivers' Motor Vehicle Records to Solicit the Drivers' Participation in Litigation Without Obtaining the Drivers' Express Consent?, PREVIEW OF UNITED STATES SUPREME COURT CASES, (c) 2013 American Bar Association

**January** 7, 2013

842. Can a Plaintiff Who Alleges Only Mental and Emotional Distress Receive "Actual Damages" Under the Privacy Act?, PREVIEW OF UNITED STATES SUPREME COURT CASES, (c) 2011 American Bar Association

**November** 28, 2011

843. Does the Freedom of Information Act's Protection for "Personal Privacy" Protect the Privacy of Corporate Entities?, PREVIEW OF UNITED STATES SUPREME COURT CASES, (c) 2011 American Bar Association

**January** 10, 2011

844. Do Questions About Drug Treatment and Counseling or Certain Open-Ended Queries Made in the Course of Employee Background Investigations Violate Federal Contract Employees' Constitutional Right to Informational Privacy?, PREVIEW OF UNITED STATES SUPREME COURT CASES, (c) 2010 American Bar Association

**October** 4, 2010

845. Does the Fourth Amendment's Right to Privacy Protect Personal Communications over a Government-Issued Pager?, PREVIEW OF UNITED STATES SUPREME COURT CASES, (c) 2010 American Bar Association

**April** 19, 2010

846. Copyright (c) 2012 American Bar Association Public Contract Law Journal, Winter, 2012, 41 Pub. Cont. L.J. 385, NOTE LOST IN THE CLOUD: PROTECTING END-USER PRIVACY IN FEDERAL CLOUD COMPUTING CONTRACTS, Joshua S. Parker

847. Copyright (c) \*\*YEAR\*\* American Bar Association The Health Lawyer, October, 2010, 23 Health Lawyer 18, IN THIS ISSUE THE USEFULNESS OF NON-LINEAR THINKING: CONCEPTUAL ANALYSIS TOOLS AND AN OPPORTUNITY TO DEVELOP ELECTRONIC HEALTH INFORMATION PRIVACY LAW <1>, Kathryn McEnery, JD, Buxbaum, Daue & Fitzpatrick, Missoula, MT

... Ct. App. Nov. 9, 2006) led to readings on the **privacy** and security portions of the Health Insurance Portability and Accountability Act of ...

... turn suggested research on the healthcare industry, the history of legal **privacy** concepts, contemporary issues in electronic health information ...

848. Copyright © 2014 University of Maryland Francis King Carey School of Law. All Rights Reserved. Journal of Business & Technology Law, 2014, Journal of Business & Technology Law, 9 J. Bus. & Tech. L. 315, 11826 words, NOTE & COMMENT: Electronic Privacy Information Center v. National Security Agency: How Glomar Responses Benefit Businesses and Provide an Epic Blow to Individuals, JOSHUA R. CHAZEN \*

849. The Cambridge Law Journal (UK), 1 July 2014, The Cambridge Law Journal, 73 [2014], pp 350-377, Beyond Information: Physical Privacy in English Law, N. A. Moreham, Associate Professor of Law, Victoria University of Wellington. I would like to thank Mark Warby QC, 5 Raymond Buildings, London; Professor Tanya Aplin, King's College London; Professor John Bell, University of Cambridge; and two anonymous peer reviewers for their helpful comments on earlier drafts. Thanks also to Steven Price, Barrister, Wellington, and participants in a joint meeting of the University of Cambridge Centre for Public Law and Torts Research Group at which an earlier version of this work was presented. I accept full responsibility for all content.

850. The Cambridge Law Journal (UK), 1 November 2013, The Cambridge Law Journal, 72 [2013], pp 504-508, Case and Comment, "Mens rea", Breach of Confidence and the Implications for England's Privacy "Tort", Chris D. L. Hunt

851. Competition Law International (IBA) Copyright © 2013 International Bar Association (IBA). All Rights Reserved., 9-2 CLI 183, October 2013, No Free Lunch: Personal Data and Privacy in EU Competition Law

852. Copyright © 2013 American Bar Association, Tort Trial & Insurance Practice Law Journal, Fall, 2013, 49 Tort & Ins. L.J. 297, 13680 words, ARTICLE., Recent Developments in Media, Privacy, and Defamation Law, John P. Borger, Emily R. Caron, Ashley Kissinger, Matthew E. Kelley, Joseph R. Larsen, Katharine Larsen, Thomas Leatherbury, Steven P. Mandell, Katherine E. Mast, Elizabeth A.F. Morris, Kristen C. Rodriguez, Leita Walker, Thomas J. Williams, Travis Wimberly, and Steven Zansberg

853. Copyright © 2013 Arizona Board of Regents. All Rights Reserved. Arizona Journal of Environmental Law & Policy, Spring, 2013, Arizona Journal of Environmental Law & Policy, 3 Ariz. J. Envtl. L. & Pol'y 141, 8545 words, ARTICLE: PRIVACY ISSUES SURROUNDING THE TRACKING AND SHARING OF BOAT MOVEMENT INFORMATION AS PART OF INVASIVE SPECIES PREVENTION PROGRAMS, Nicole Giffin \*

854. Copyright (c) 2013 American Bar Association Communications Lawyer, June, 2013, 29 Comm. Lawyer 1, MOBILE PRIVACY INITIATIVES AND ACTIONS CLOUD THE FUTURE, CREATING A PATCHWORK LANDSCAPE OF POLICY AND REGULATORY PROSPECTS, Mary Ellen Callahan, Michael T. Borgia, David M. Didion, and Sabrina N. Guenther

855. Copyright © 2014 American Bar Association, The International Lawyer, Spring, 2013, 47 Int'l Law. 99, 8077 words, BUSINESS REGULATION., Privacy, E-Commerce, and Data Security, W. Gregory Voss, Katherine Woodcock, Rob Corbet, Jan Dhont, Bruce A. McDonald, Demetrios Eleftheriou, Emily Hay, Cecil Saehoon Chung, and Jae Hyun Park \*

856. human rights, March, 2013, 39 Human Rights 6, PROTECTING CHILDREN'S PRIVACY ONLINE THE BATTLE CONTINUES, By Kathryn C. Montgomery

857. human rights, March, 2013, 39 Human Rights 7, PROTECTING PRIVACY THE ROLE OF THE COURTS AND CONGRESS, By Marc Rotenberg and David Brody

858. human rights, March, 2013, 39 Human Rights 12, EMPLOYMENT PRIVACY IS THERE ANYTHING LEFT?, By Lewis Maltby

859. human rights, March, 2013, 39 Human Rights 22, PRIVACY IN HOLLYWOOD?, By Alexander Wohl

860. Copyright (c) 2012 American Bar Association Communications Lawyer, November, 2012, 29 Comm. Lawyer 10, CYBERPRIVACY AND DIGITAL PRIVACY RISKS, Blaine Kimrey and Bryan Clark

861. Copyright © 2012 American Bar Association ABA: Antitrust Source, October, 2012, 12-1 Antitrust Src. 1, THE FTC AND PRIVACY: WE DON'T NEED NO STINKING DATA, THOMAS M. LENARD AND PAUL H. RUBIN

862. Copyright © 2012 American Bar Association, Tort Trial & Insurance Practice Law Journal, Fall, 2012, 48 Tort & Ins. L.J. 359, 15553 words, ARTICLE., RECENT DEVELOPMENTS IN MEDIA, PRIVACY, AND DEFAMATION LAW, John P. Borger, Patrick L. Groshong, Ashley Kissinger, Joseph R. Larsen, Katharine Larsen, Thomas Leatherbury, Steven P. Mandell, Katherine E. Mast, Elizabeth A.F. Morris, Leita Walker, Thomas J. Williams, Travis Wimberly, and Steven D. Zansberg

863. Copyright © 2012 Temple University School of Law. All Rights Reserved. American Journal of Legal History, April, 2012, American Journal of Legal History, 52 Am. J. Legal Hist. 183, 8019 words, ARTICLE: The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law, by BERNARDO PERINAN \*

864. Copyright © 2012 American Bar Association, The International Lawyer, Spring, 2012, 46 Int'l Law. 97, 9385 words, BUSINESS REGULATION., Privacy, E-Commerce, and Data Security, W. GREGORY VOSS, KATHERINE WOODCOCK, DAVID DUMONT, NICHOLAS D. WELLS, JONATHAN I. EXOR, JOAO LUIS TRACA, BERNARDO EMBRY, AND FATIMA KHAN \*

865. Competition Law International (IBA) Copyright © 2011 International Bar Association (IBA). All Rights Reserved., 7-2 CLI 59, November 2011, Antitrust and Privacy

866. Competition Law International (IBA) Copyright © 2011 International Bar Association (IBA). All Rights Reserved., 7-2 CLI 60, November 2011, Internet Intermediaries, Cloud Computing and Geospatial Data: How Competition and Privacy Converge in the Mobile Environment

867. Dispute Resolution International (IBA) Copyright © 2011 International Bar Association (IBA). All Rights Reserved., 5 DRI 127, November 2011, European and German Privacy Laws and Cross-Border Data Transfer in US Discovery Procedures

868. The Cambridge Law Journal (UK), 1 November 2011, The Cambridge Law Journal, 70 [2011], pp 489-491, Strasbourg on privacy injunctions, Chris Hunt

869. Copyright (c) 2011 American Bar Association Communications Lawyer, November, 2011, 28 Comm. Lawyer 1, PRIVACY EXPECTATIONS IN ONLINE SOCIAL MEDIA--AN EMERGING GENERATIONAL DIVIDE?, Steven D. Zansberg and Janna K. Fischer

870. Copyright © 2011 American Bar Association, Tort Trial & Insurance Practice Law Journal, Fall, 2011, 47 Tort & Ins. L.J. 359, 16421 words, ARTICLE., RECENT DEVELOPMENTS IN MEDIA, PRIVACY, AND DEFAMATION LAW, Shari Albrecht, John P. Borger, Patrick L. Groshong, Ashley Kissinger, Joseph R. Larsen, Katharine Larsen, Thomas Leatherbury, Steven P. Mandell, Katherine E. Mast, Catherine Van Horn, Leita Walker, Thomas J. Williams, and Steven Zansberg

871. Copyright © 2011 Temple University School of Law. All Rights Reserved. American Journal of Legal History, July, 2011, American Journal of Legal History, 51 Am. J. Legal Hist. 461, 18855 words, ARTICLE: Privacy and Prurience: An Essay on American Law, Religion, and Women \*, by MARIE ASHE \*\*

872. Copyright © 2011 New York University School of Law. All Rights Reserved. New York University Intellectual Property & Entertainment Law Ledger, Spring, 2011, New York University Intellectual Property & Entertainment Law Ledger, 2 N.Y.U. Intell. Prop. & Ent. Law Ledger 107, 5356 words, ARTICLE: IS FACEBOOK KILLING PRIVACY SOFTLY? THE IMPACT OF FACEBOOK'S DEFAULT PRIVACY SETTINGS ON ONLINE PRIVACY, MICHAEL J. KASDAN \*

873. Copyright © 2011 Melbourne Journal of International Law Inc. All Rights Reserved. Melbourne Journal of International Law, June, 2011, Melbourne Journal of International Law, 12 Melbourne J. of Int'l Law 141, 20347 words, ARTICLE: WTO-COMPLIANT PROTECTION OF FUNDAMENTAL RIGHTS: LESSONS FROM THE EU PRIVACY DIRECTIVE, CARLA L REYES \*

874. Copyright © 2011 Indiana State Bar Association. All Rights Reserved. Res Gestae Indiana Bar Journal, May, 2011, 54 Res Gestae 129, 2067 words, DEPARTMENT: ETHICS CURBSTONE: THE ZONE OF PERSONAL PRIVACY FOR JUDGES AND LAWYERS, By Donald R. Lundberg

875. The Cambridge Law Journal (UK), 1 March 2011, The Cambridge Law Journal, 70 [2011], pp 31-34, Family Abuse, Privacy and State Intervention, Jo Miles

876. human rights, Winter, 2011, 38 Human Rights 5, PRIVACY AND SURVEILLANCE POST-9/11, By Hina Shamsi and Alex Abdo

877. Law and History Review (UK), 1 November 2010, Law and History Review November 2010, Vol. 28, No. 4, 1080-1082, Book Reviews: Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy, Norman L. Rosenberg, Macalester College

878. Copyright 2010 American Bar Association, Tort Trial & Insurance Practice Law Journal, Winter, 2010, 45 Tort & Ins. L.J. 465, 15312 words, ARTICLE., RECENT DEVELOPMENTS IN MEDIA, PRIVACY, AND DEFAMATION LAW, John P. Borger, Jay Ward Brown, B. Gerard Cordelli, F.M. Bud Ferrer, Kourtney James, Ashley Kissinger, D. Bradley Kizzia, Joseph Larsen, Thomas Leatherbury, Katherine E. Mast, John B. O'Keefe, Catherine Van Horn, Leita Walker, Natalie West, Thomas J. Williams, and Steven Zansberg

879. Copyright © 2013 Indiana State Bar Association. All Rights Reserved. Res Gestae Indiana Bar Journal, January/February, 2013, 56 Res Gestae 28, 5765 words, FEATURE: 'INTRUSION' INTO PRIVACY -- HOW INDIANA VEERED OFF COURSE, AND HOW IT CAN GET BACK ON TRACK, By Neal F. Eggeson

880. The Army Lawyer, April, 2013, The Army Lawyer, 2013 Army Law. 3, 35768 words, ARTICLE: An Introduction to Intelligence Oversight and Sensitive Information: The Department of Defense Rules for Protecting Americans' Information and Privacy, Kevin W. Kapitan \*

881. Copyright © 2013, The American Bar Association The Urban Lawyer, Winter, 2013, 45 Urb. Law. 203, ARTICLE: EDUCATION LAW SYMPOSIUM: Student Rights: Book 'em?: Navigating Student Privacy, Disability, and Civil Rights and School Safety in the Context of School-Police Cooperation, Lynn M. Daggett\*

882. Copyright (c) 2013 North Caolina Journal of Law & Technology, Online Edition. All Rights Reserved. North Carolina Journal of Law & Technology, Online Edition, 2013, North Carolina Journal of Law & Technology, Online Edition, 14 N.C. J.L. & Tech. On. 167, 14331 words, ARTICLE: CHILDREN'S PRIVACY IN VIRTUAL K-12 EDUCATION: VIRTUAL SOLUTIONS OF THE AMENDED CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA) RULE, David R. Hostetler \* & Seiko F. Okada \*\*

883. Copyright (c) 2013 North Caolina Journal of Law & Technology, Online Edition. All Rights Reserved. North Carolina Journal of Law & Technology, Online Edition, 2013, North Carolina Journal of Law & Technology, Online Edition, 14 N.C. J.L. & Tech. On. 205, 16536 words, ARTICLE: STEALING GLANCES: ELECTRONIC COMMUNICATIONS PRIVACY AND THE NECESSITY FOR NEW LEGISLATION IN THE DIGITAL AGE, Laura Arredondo-Santisteban \*

884. Copyright (c) 2010 North Caolina Journal of Law & Technology, Online Edition. All Rights Reserved. North Carolina Journal of Law & Technology, Online Edition, June, 2010, North Carolina Journal of Law & Technology, Online Edition, 11 N.C. J.L. & Tech. On. 259, 10350 words, ARTICLE: "APPS.GOV": ASSESSING PRIVACY IN THE CLOUD COMPUTING ERA, Shahid Khan \*

885. Copyright © 2014 Wake Forest University School of Law. All Rights Reserved. Wake Forest Journal of Law & Policy, April, 2014, Wake Forest Journal of Law & Policy, 4 Wake Forest J. L. & Pol'y 257, 9833 words, COMMENT: NO WARRANTS SHALL ISSUE BUT UPON PROBABLE CAUSE: THE IMPACT OF THE STORED COMMUNICATIONS ACT ON PRIVACY EXPECTATIONS, ERIK E. HAWKINS +

886. Copyright (c) 2011 American University Labor & Employment Law Forum. All Rights Reserved. American University Labor & Employment Law Forum, Winter, 2011, American University Labor & Employment Law Forum, 1 Am. U. Labor & Emp. L.F. 27, 16825 words, ARTICLE: PRIVATE ORDERING OF EMPLOYEE PRIVACY: PROTECTING EMPLOYEES' EXPECTATIONS OF PRIVACY WITH IMPLIED-IN-FACT CONTRACT RIGHTS, LINDSAY NOYCE \*

887. ALI-ABA COURSE OF STUDY MATERIALS , Investment Company Regulation and Compliance, June 2010, SR028, PRIVACY, By Robert G. Bagnall n1

888. ALI-ABA COURSE OF STUDY MATERIALS , Fundamentals of Employee Benefits Law, April 2011, SS030, 28769 words, EMPLOYER-SPONSORED HEALTH PLANS UNDER NON-PRIVACY HEALTH PLAN PROVISIONS OF HIPAA Copyright (c) 2011 Roberta Casper Watson and Douglass A. Farmsworth. All rights reserved, By Roberta Casper Watson and Douglass A. Farnsworth n1

889. ALI-ABA COURSE OF STUDY MATERIALS , Investment Company Regulation and Compliance, July 2011, ST007, 7579 words, PRIVACY, By Thomas S. Harman n1

890. ALI-ABA COURSE OF STUDY MATERIALS , Current Developments in Employment Law: The Obama Years at Mid-Term Volume 2, July 2011, ST001, 41497 words, SOCIAL MEDIA AND PRIVACY IN THE WORKPLACE (c) 2011 Robert B. Fitzpatrick, PLLC. All Rights Reserved., By Robert B. Fitzpatrick

891. ALI-ABA COURSE OF STUDY MATERIALS , Legal Issues in Museum Administration Cosponsored by The Smithsonian Institution with the cooperation of the American Association of Museums, March 2012, ST024, 32405 words, CREATING AND MANAGING BRAND AND CONTENT ON THE WEB (COPYRIGHT, TRADEMARK, AND PRIVACY ISSUES), Submitted by Karen S. Frank and Lauryn H. Guttenplan and Nate A. Garhart, Esquire and Walter G. Lehmann

892. ALI CLE COURSE OF STUDY MATERIALS , Employee Benefits Law and Practice Update: Spring 2012, May 2012, VCT0509, 39568 words, SELECTED MATERIALS ON HIPPA PRIVACY REGULATIONS, [NO AUTHOR IN ORIGINAL]

893. ALI CLE COURSE OF STUDY MATERIALS , Fundamentals of Employee Benefits Law, May 2012, ST043, 28766 words, EMPLOYER-SPONSORED HEALTH PLANS UNDER NON-PRIVACY HEALTH PLAN PROVISIONS OF HIPAA Copyright (c) 2011 Roberta Casper Watson and Douglass A. Farnsworth. All rights reserved, By Roberta Casper Watson And Douglass A. Farnsworth n1

894. ALI CLE COURSE OF STUDY MATERIALS , Health Plans Update: When It Rains, It Pours. Dealing with Health Reform's Tsunami, February 2013, VCU0220, 46554 words, HIPAA'S PRIVACY REGULATIONS, HITECH, AND THEIR IMPACT ON GROUP HEALTH PLANS (C) 2013 Greta E. Cowart. All Rights Reserved, By Greta E. Cowart

895. ALI CLE COURSE OF STUDY MATERIALS , Pension, Profit-Sharing, Welfare and Other Compensation Plans, March 2013, SU039, 327 words, HHS RELEASES FINAL OMNIBUS HIPAA PRIVACY AND SECURITY REGULATIONS, By Tamara M. Simon

896. ALI CLE COURSE OF STUDY MATERIALS , Pension, Profit-Sharing, Welfare and Other Compensation Plans, March 2013, SU039, 5218 words, HHS RELEASES FINAL OMNIBUS HIPAA PRIVACY AND SECURITY REGULATIONS, By Tamara M. Simon

897. ALI CLE COURSE OF STUDY MATERIALS , Retirement, Deferred Compensation, and Welfare Plans of Tax-Exempt and Governmental Employers, September 2013, SV006, 46579 words, HIPAA'S PRIVACY REGULATIONS, HITECH AND THEIR IMPACT ON GROUP HEALTH PLANS Copyright © 2013 Greta E. Coward. All Rights Reserved, By Greta E. Cowart

898. ALI CLE COURSE OF STUDY MATERIALS , Retirement, Deferred Compensation, and Welfare Plans of Tax-Exempt and Governmental Employers, September 2013, SV006, 2928 words, HIPAA PRIVACY AND SECURITY OMNIBUS REGULATION CHANGES Copyright © 2013 Greta E. Coward. All Rights Reserved, By Greta E. Cowart

899. ALI CLE COURSE OF STUDY MATERIALS , Pension, Profit-Sharing, Welfare, and Other Compensation Plans, October 2013, SV007, 46585 words, HIPAA'S PRIVACY REGULATIONS, HITECH AND THEIR IMPACT ON GROUP HEALTH PLANS Copyright © 2013 Greta E. Cowart. All Rights Reserved, By Greta E. Cowart

900. ALI CLE COURSE OF STUDY MATERIALS , Pension, Profit-Sharing, Welfare, and Other Compensation Plans, October 2013, SV007, 2929 words, HIPAA PRIVACY AND SECURITY OMNIBUS REGULATION CHANGES Copyright © 2013 Greta E. Cowart. All Rights Reserved, By Greta E. Cowart