Data privacy and data protection: US law and legislation

An ESET White Paper
by
Stephen Cobb, CISSP

Abstract: *Over the last four decades, the privacy of personal data has been the subject of legislation and litigation in both the US and the EU. Protection of personal data privacy under the law has been shaped by the interests of multiple constituencies: individuals, commercial organizations, government agencies, law enforcement, and national security services. This white paper examines the development of data privacy legislation in the US as an ongoing balancing act, with security interests on one side, and the interest of the individual on the other. The complex and arguably incomplete nature of US data privacy law is often criticized by countries that have more comprehensive data protection legislation. Yet that very complexity can obscure some data privacy protections that are then overlooked by critics. The paper serves to provide a neutral review of US data privacy legislation; however, it also observes that interests other than those of the individual have tended to prevail in US data privacy legislation, notably the interests of commerce, as well as those of state security agencies, particularly those that respond to the complex technical realities of data communication and data processing with a "collect everything" approach to electronic surveillance.*

As the use of computerized databases to store information about individuals became widespread in Europe and the Americas in the 1970s, data protection legislation began to appear (Cate, 1995; Regan, 1984). The rapid uptake of this new information technology by government agencies and businesses sparked fears of potentially deleterious effects, such as errors in the data or secret surveillance by the state or commercial entities, all of which had potentially chilling effects on individual privacy and personal freedoms. Elected representatives seeking to protect their constituents from the potential harms of data processing formulated legislative solutions. The term "data protection" was coined in Europe to describe privacy-protective legislation while in the United States (US) this effort was more commonly referred to as data privacy (Swire and Ahmad, 2012a).

As legislative protection for the privacy of data pertaining to people has evolved during the last four decades it has attempted to accommodate the interests of numerous constituencies: individuals, commercial organizations, government agencies, law enforcement, and national security services. This white paper examines the development of privacy legislation in the US as an ongoing balancing act, with security interests on one side, and the interest of the individual on the other.

The complex and arguably incomplete nature of US data privacy law is often criticized by countries that have more comprehensive data protection legislation (Bignami, 2007). This paper suggests that interests other than those of the individual have tended to prevail in US privacy legislation, notably the interests of commerce and those of state security agencies committed to a "collect everything" approach to electronic surveillance (Robinson, 2014). After reviewing US data privacy legislation from the perspective both of the individual and of security interests, the paper will highlight factors that continue to prevent it from achieving an appropriate balance between the two.

HEW are you?

Ever since the US Department of Health, Education, and Welfare (HEW) published the 1973 report titled *Computers and the Rights of Citizens*, a complex array of legal instruments has evolved in the US to protect individuals from 'harmful consequences that might result from automated personal data systems' (Ware, 1973: 1). More commonly referred to as privacy protection than data protection in the US, these instruments include laws, case law, and constitutional rights. The last of these are overseen by a tripartite system of checks and balances, created by the three separate but equal branches of US government: legislative, executive, and judicial (Swire and Ahmad, 2012b).

The first US legislation specifically addressing the harmful consequences of personal data held in computerized databases was the Fair Credit Reporting Act of 1970. Often referred to by its initials – a common practice in US legal discourse – FCRA was passed to reform the consumer credit reporting industry, imposing limits on data sharing and making it easier for individuals to correct errors, the consequences of which could be severe. Many Americans might be surprised to know that the first US president to highlight these issues was Richard Nixon. For example, in February of 1974 Nixon gave a radio address titled 'About the American Right of Privacy' from which it was clear that he understood how information technology's dark side could extend far beyond financial damage due to erroneous credit data. Nixon talked about careers being ruined and worse: 'marriages have been wrecked, reputations built up over a lifetime have been destroyed by the misuse or abuse of data technology in both private and public hands' (1974: n.p.).

FCRA established a model for future US data protection legislation. First, address the interest of individual citizens by providing notice of, and consent to, a specific type of personal data record. Second, establish an administrative procedure for individual redress administered by a specified agency (for FCRA, that agency is the FTC, the Federal Trade Commission). Third, address the interests of law enforcement and national security by defining the terms and conditions under which protected data can be accessed. These include the scope and purpose of the requested access plus the desired level of justification. The latter can range from a "Fourth Amendment warrant" supported by probable cause, down to a subpoena drafted by an attorney or police officer, or even a simple written request from an agency administrator.

In that 1974 radio address on privacy, Nixon took credit for FCRA and other key developments in data privacy such as the above-referenced HEW Report that recommended enshrining in law a Code of Fair Information Practices (FIPs) to which all organizations with

personal data systems would be required to adhere (Lin and Millett, 2007; Waldo, 2007; Gellman, 2014). The report envisioned that, once the code of practices was in place, any handling of personally identifiable information that did not abide by the code should be deemed unfair and thus subject to government sanction, as well as grounds for redress by individuals adversely affected (Ware, 1973). The five practices spelled out in the report ban secret databases of personal information, mandate access to data about oneself, forbid use of personal data without consent for purposes other those for which they were collected, require a way to correct information about oneself, and impose a duty of care to protect personal data from abuse or misuse (Ware, 1973).

The influence of the HEW FIPs can be detected in data privacy developments outside the US, such as the 1980 OECD data privacy guidelines (OECD, 2013) and the 1981 Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (COE, 1981). In turn, the COE Convention shaped the primary EU legal instrument on data protection: Directive 95/46/EC (EU, 1995; COE-FRA, 2012; Ahmadi and Swire, 2012b). These foundational documents not only formalized the principle that all personal data be protected by default, but provided several helpful terms of art: data subject, 'an individual who is the subject of personal data' (ICO, 2015); and data controller, 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data' (EU, 1995: 2a).

With fair information practices for all?

The US went ahead and embodied the FIPs in the Privacy Act of 1974 (PA) but whereas the HEW Report envisioned a law that applied to 'all automated personal data systems' (Ware, 1973: 5), the final version limited the scope of the legislation to federal agency databases (Regan, 1984). This limitation was a major victory for lobbyists representing commercial interests. They had argued – and they continue to assert today – that including private sector data controllers in a comprehensive regime of data privacy protection stifles trade and unfairly burdens businesses (Regan, 1984).

A counter argument might be to consider California, which has the strictest data privacy laws of any state, yet it is the most consistently prosperous and innovative of them all (Coplan 2015; Kirkham, 2016). Nevertheless, lobbyists have always succeeded in preventing expansion of Privacy Act protection to commercial data controllers, solidifying the divergence between US and European approaches to privacy protection (Bennett, 1992; Bignami, 2007). The argument that individual data privacy is well-served by commercial would seem to be undermined by the apparent inability of many companies to prevent the exposure of personally identifiable data that they are processing and storing (PRC, 2015). Unfortunately, government agencies have also proven to be "breach-prone" as well (GAO, 2015), even before the massive Office of Personnel Management breach (Loten, 2015).

The US approach to protecting data privacy – addressing specific categories of data with specific laws – continued through the 1970s with the Family Educational Rights and Privacy Act of 1974 (FERPA), which addressed the privacy of student education records. FERPA oversight was assigned to the Department of Education. Law enforcement access to data

protected by FERPA requires a judicial order or a lawfully issued subpoena, a higher threshold than some other US privacy legislation; however, as Murphy has noted, the value to security and law enforcement of FERPA data is somewhat limited (2013).

The privacy of personal banking and accounting records was addressed by the Right to Financial Privacy Act of 1978 (RFPA). Oversight of RFPA lies with the US Department of Treasury. The law has been amended several times to enable law enforcement to more easily access protected financial information, and to promote bank reporting to the authorities, notably through a Suspicious Activity Report (SAR) filed with Treasury's Financial Crimes Enforcement Network. RFPA is notable as the first of a number of sectoral privacy laws to be passed in reaction to decisions handed down by the Supreme Court of the United States (SCOTUS).

As the primary institution within the third branch of government – the judiciary – SCOTUS interprets the US Constitution, the foundation of all government institutions in the country's particular form of constitutional democracy (Chemerinsky, 2014; Habermas and Rehg, 2001). SCOTUS has played a significant role in balancing the interests of security and individual privacy because no explicit right of privacy is asserted in the US Constitution (nor in the Bill of Rights, incorporated into the Constitution in 1791 through the Tenth Amendment). However, according to Peltz-Steele, privacy within the Constitution is 'manifested as a constitutional value' (2015: 17), most notably as 'the right to be left alone' described by Justice Brandeis' dissenting opinion in *Olmstead v. United States*. This right is derived from the Fourth Amendment assertion 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 … particularly describing the place to be searched, and the persons or things to be seized' (US Const. amend. IV).

The lack of comprehensive US data privacy legislation has placed the Fourth Amendment at the heart of much privacy litigation. Privacy advocates and defense attorneys alike seek to uphold "probable cause warrants" as the baseline requirement for any searches of personal data records, but judicial interpretation of the Fourth Amendment has been hard to predict in cases where personal information is either processed in digital form, or outside the home, or by a third party (Pell and Soghoian, 2015).

Legislators passed RFPA in the wake of two SCOTUS decisions. In *United States v. Miller*, the Fourth Amendment expectation of privacy with respect to personal bank records was arguably undermined by the data subject sharing the information with a third party, namely his bank. Known as the "third party doctrine" this is the same argument that is used to deny privacy to personal records placed outside the home as trash for pickup, or to information about phone calls handled by the phone company. The other SCOTUS decision motivating passage of RFPA was the finding in *Fisher v. United States* that individuals have no grounds to refuse to reveal records of their private financial affairs under the Fifth Amendment right against self-incrimination *if an accountant maintains those records*. RFPA countered SCOTUS by extending protection to accounts maintained by a third party.

How about a side order of privacy?

The absence of US legislation that explicitly protects the interests of data subjects by default has led to protection being tacked onto sector-specific legislation, notably that which is prompted by new technology. For example, the emergence of the cable TV industry prompted passage of the Cable Communications Policy Act of 1984 (CCPA). Lawmakers bundled basic privacy protections for subscriber data in with the policies.

The video tape rental business sparked the Video Privacy Protection Act of 1988 (VPPA) when congressional representatives realized how embarrassing the revelation of an individual's rental records could be. This realization dawned after public disclosure of such records pertaining to Judge Robert H. Bork during his Supreme Court confirmation hearings (Halpert and White, 2013). As in many of these sector or technology specific statutes, VPPA contains a law enforcement agency exception: 'pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order' with the last of these being a fairly low barrier to access.

The VPPA has since been amended to reflect the rise of online video content rentals. Industry interests have argued that disclosure of information pertaining to content on services like Netflix is more complex to manage, and that obtaining consent to disclose a person's viewing activity on a per item basis is more problematic than it was with physical tape and disc rentals (Halpert and White, 2013). These arguments would appear to arise from concerns over regulatory and litigation risks, although privacy advocates are concerned about 'the interaction of the VPPA with the recent Patriot Act, which expanded law enforcement powers to procure information such as library records and individual purchasing records "in the course of an ongoing investigation" (a lower standard than the traditional warrant)' (EPIC, 2016).

The Gramm-Leach-Bliley Act of 1999 (GLBA) was passed to deregulate the banking and financial services sector but included a Financial Privacy Rule to promote fair information practices in the marketing of financial services. Enforcement of GLBA was assigned to the FTC and security interests were addressed by requiring financial institutions to cooperate with civil, criminal, or regulatory investigations. A subpoena or summons by Federal, state or local authorities was mandated for access to protected data. At the same time, GLBA banned a technique that private investigators have been known to use: pretexting, a form of social engineering used to gain access to a person's private financial data without their knowledge or permission. The use of similar techniques to obtain personal phone records was explicitly banned by the Telephone Records and Privacy Protection Act of 2006 (TRPPA).

Data privacy as a side effect of industry reform is epitomized by the legislation that protects a particularly sensitive type of data: personal health information. With certain exceptions, data of this type is protected in the US by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of HIPAA was to improve employment-based health insurance coverage (Swire and Ahmad, 2012b). However, commercial interests – notably insurance companies – claimed that this would be too costly, so provisions to promote the adoption of cost-saving electronic transactions by the healthcare industry were added.

Given that such adoption would greatly expand the computerized processing of personal health information, legislators mandated protections for this data in HIPAA, ultimately assigning rule making and enforcement to the Department of Health and Human Services (HHS). The department's Office of Civil Rights (OCR) investigates exposures of Protected Health Information (PHI) alleged by individuals and levies fines for violations. In 2015 these totaled over $6 million (Snell, 2015). In another nod to commercial interests, HIPAA does not provide an individual right of action. Furthermore, HIPAA illustrates how the practice of applying data protection as part of industry regulation can lead to loopholes: doctors who operate on a cash basis are not required to comply.

Three more acts round out this review of US data protection legislation: the Driver's Privacy Protection Act of 1994 (DPPA); the Children's Online Privacy Protection Act of 1998 (COPPA); and the Genetic Information Nondiscrimination Act of 2008 (GINA). Like the other acts, these all provide for law enforcement access to protected data.

States of privacy and the FTC

By now it should be clear that, while the privacy interests of individuals in the US are protected in a wide range of situations, the protection is far from universal. For example, there is no explicit federal privacy protection for an individual's airline reservation data or library borrowing records. Whole categories of data – like the customer and prospect databases widely used in sales and marketing – lack explicit protection under federal law, despite the fact that unauthorized access to them is potentially harmful to the data subjects. Such gaps have led some privacy advocates to make unfavorable comparisons between US data protection legislation and that of European countries where all personal data is protected by default and there is a national office of data protection to whom individuals can turn for redress (Bignami, 2007). Such criticism may be warranted, but some critics (Baumer, Earp and Poindexter, 2004; Bennett, 2011) are apt to underestimate one or more of the three aspects of US privacy protection not yet reviewed: state laws; the FTC's role as America's privacy watchdog; and case law.

Many of America's 50 states have passed legislation mandating stronger protection of personal information than the federal government requires. Each state in the union has its own constitution and 10 of these include an explicit right of privacy (National Conference of State Legislatures, 2015a). In addition, almost all states – 47 as of the end of 2015 – have laws that address the individual's interest in knowing when the security of her data has been breached (National Conference of State Legislatures, 2015b). Some state privacy laws apply to all industry sectors and all types of personal data, others fill gaps in federal protection; for example, almost all states offer protection for library records (American Library Association, 2015). Some states have gone further than the federal government in emerging areas of data protection (National Conference of State Legislatures, 2015c). For example, California has already outlawed warrantless use of Stingrays, surveillance technology discussed later in this paper (Farivar, 2015). One effect of these state laws is to complicate efforts by other countries to evaluate privacy protection in the US.

Another factor complicating efforts by other countries to evaluate the level of data protection afforded individuals in the US is the FTC's role in policing consumer privacy; after

all, there is nothing in the name Federal Trade Commission that suggests a focus on either privacy. Furthermore, there is no mention of privacy in the legislation under which that FTC role has evolved. The Federal Trade Commission Act of 1914 (FTCA, as amended by the Wheeler-Lea Act of 1938) charged the agency with protecting businesses and consumers from unfair competition and unfair or deceptive commercial practices (Rubinstein, 2011; Solove and Hartzog, 2014).

The FTC's emergence as the leading defender of the data privacy interests of individuals, shaping consumer privacy and commercial data security practices over the last 15 years, is well documented (Murphy, 2013; Serwin, 2014; Stevens, 2014). Along the way the agency has imposed numerous legal settlements, levied millions of dollars in fines, and overseen monetary reimbursements to consumers. A brief review of an early FTC action will illustrate the two legal doctrines by which the agency pursues its data privacy remit. The case of *FTC v. Eli Lilly* was settled in 2002 after the agency alleged that the pharmaceutical company failed to follow responsible code development practices and thereby exposed the identity of people who had expressed an interest in Prozac, an anti-depressant medication (FTC, 2002).

The breach of personally identifiable information resulted from a programming error. Research commissioned by the FTC and performed by the author and colleagues, determined that this error would have been remediated if standard IT practices – including preproduction testing – had been followed. While such practices were stipulated in the company's own policies, research indicated that these policies had not yet been applied to web- and email-based marketing activities (Cobb, 2003). From the FTC's perspective, Lilly was culpable firstly of deceiving consumers by assuring them on its website that their interest in Prozac, and their personally identifiable information, would be kept private and secure. The FTC argued that such assurances to the data subjects were material to their decision to provide that information. Secondly, it was alleged that, by failing to live up to those privacy promises, Eli Lilly potentially caused harm to the persons who were exposed (Cobb, 2002).

FTC cases are usually settled with no admission of wrongdoing by defendants. This might sound like a soft touch, but FTC consent orders – most of which follow the template forged in the Lilly case – impose a serious compliance burden. The FTC often requires the defendant to establish and execute a program of improvements to its data privacy and system security practices. The progress of this program is then subject to periodic outside audits by independent parties – such as CISSPs – for the length of the settlement period, which can be as long as 20 years. Furthermore, defendants must agree to pay fines to the FTC if the consent order is violated at any time during that period. For example, when the FTC determined that Lifelock, a vendor of identity protection services, had violated its 2010 consent order, the company had to pay a $100 million fine (FTC, 2015a).

The FTC clearly addresses some of the data privacy interests of individuals. Case law like *FTC v. Wyndham* has established the agency's authority in the courts (FTC, 2015b; Serwin, 2015). However, the doctrine of harm that the agency has developed is not without problems, as Serwin suggests (2011). Absent a universal right to informational privacy, violation of which is defined as harmful, commercial data controllers culpable in a breach can argue there is no harm to the data subjects whose records have been exposed, unless they suffer a financial loss directly attributable to the breach. So far, US courts have been reluctant to agree that

the distress of a criminal possessing an individual's personal details is in itself appropriately harmful. However, case law is continually evolving and the tort of intrusion upon seclusion has been successfully applied in Canadian data breach cases (Simard and Griffin, 2014). It is possible that similar cases could gain traction in the US at some point.

Closing arguments

Despite the many different forms that data privacy protection may take in the US, the argument can still be made that the individual interest is ill served by the current state of US data protection law. But do the interests of those charged with the security of the nation and the organizations within it fare any better? It would seem so, given that various US privacy laws provide for access to "private" data by law enforcement officers, lawyers, or even data brokers that offer security management services like background checks (Bignami, 2011). However, it could be argued that the absence of a centralized federal data protection regime imposes a burden of legal complexity on anyone seeking access to protected data, whether an office of the law or a security manager for a commercial entity.

Consider this scenario: a security manager at a healthcare organization in California is asked by law enforcement to assist in the investigation of possible billing fraud by a former employee. Multiple state and federal privacy laws apply, each with its own standards and procedures for accessing protected data. The legal costs are likely to be considerable. The healthcare organization will consult counsel to avoid exposure to lawsuits. The law enforcement agency will also need counsel to minimize potential technical challenges to any fraud case that is brought as a result of the investigation. Furthermore, the existence of multiple regulatory regimes can create considerable compliance risks for organization. For example, if that former hospital employee had compromised protected health information (PHI), that could trigger an OCR audit under HIPAA. Fines in the millions could be imposed if the hospital was found to be in violation of HIPAA rules or state laws pertaining to the protection of medical data (Dvorak, 2016).

At the organizational level, current US privacy legislation imposes twin burdens of complexity and compliance on security managers. These burdens are arguably greater still when it comes to the security interests of law enforcement and state security. The apparent ease of access to some private data for authorized purposes described earlier is offset by the lack of consistency between sectoral protections, as well as between state and federal laws. This situation is further complicated by a lack of consistency between judicial interpretations of federal and constitutional law in different parts of the country. The legal status of one particular piece of data technology serves to illustrate these problems.

For nearly two decades, technology known as a Cell Site Simulator (CSS) has been used by some US law enforcement agencies to gather personal data via man-in-the-middle attacks on mobile phones (Owsley, 2014; EPIC, 2015). Sometimes called Stingrays after a popular CSS product, these suitcase-sized devices can capture nearby mobile phone traffic by pretending to be normal cellular radio towers. CSS technology can determine each mobile phone's number, the numbers it has dialed, plus the content of its communications: calls, texts, and web pages visited (Pell and Soghoian, 2014). A Stingray can do this at scale, to all nearby devices that are currently powered on, and without the knowledge of phone users or service

providers. Stingrays can clearly assist law enforcement in tracking down known or suspected criminals. They can also help the security services conduct the kind of pre-emptive surveillance that some see as essential to protecting the US against terrorists who have embraced suicide attacks (Goede, 2014; Mitsilegas, 2015).

Ironically, the beneficial use of these devices in the interests of security has been hampered by five different factors currently affecting privacy and the law in the US. Firstly, CSS manufacturers themselves, while seeking to sell a technology, have tried to limit knowledge of the technology's use, presumably because it might not reflect well on the corporate image. Consequently, CSS makers have attempted to contractually limit any mention of their deployment. According to Brown and Leese (2015) criminal cases have been lost because law enforcement officers called as prosecution witnesses would not reveal the source of key evidence because it was from a Stingray.

Secondly, it can be argued that certain dubious practices have limited the benefits of CSS technology, due in part to law enforcement's need to rely on centuries' old constitutional guidance and decades' old case law to determine the status of privacy invasive searches performed with new technology. According to Owsley (2014) and Brown and Leese (2015), some law enforcement agencies avoided warrants for Stingrays entirely rather than be denied. Others persuaded judges to authorize their use as though they were equivalent to older and much more limited telephone surveillance technology known as pen registers. Thirdly, as the Snowden revelations of mass electronic surveillance in 2013 made clear, the three branches of government have failed to provide adequate checks and balances on security interests (Gutierrez, 2014; Lyon, 2015; Ombres, 2015). Congressional gridlock has stymied passage of new privacy legislation. An environment has been allowed to evolve in which warrantless searches, such as those sometimes performed with Stingrays, are secretly sanctioned. The situation has been exacerbated by presidential use of executive orders such as EO 12,333 to bypass legislative and judicial privacy protections, (Bloom and Dunn, 2006; Newland, 2015).

The fourth factor hampering legitimate use of surveillance technologies is lack of consensus as to the proportionality of the security service response to threats to the nation. Clearly there is a genuine terrorist threat that needs to be addressed, but warrantless mass electronic surveillance may not be the most effective response. While voices have been raised in defense of the government's actions (Etzioni, 2015), many in the judiciary and academy have been deeply critical, arguing that the security response has been excessive, disproportionate, and deleterious (Chemerinsky, 2009; Reidenberg, 2014; Robinson, 2014). The fifth complicating factor is the absence of comprehensive unified data protection legislation. That leaves many data privacy grey areas, which in turn create far too much latitude for anyone seeking to use an individual's data without notice or consent, whether for profit or protection of the nation (Bignami, 2007).

As Cate, Dempsey and Rubinstein (2012) have demonstrated, it would be naïve to think that European-style data protection legislation alone can prevent surveillance of the citizenry by its security services at levels widely perceived as invasive and disproportionate to threat levels. Both Brown (2012) and Koops (2014) reveal serious shortcomings in European-style data protection in multiple countries. However, on balance it is hard to argue with Bignami

(2007) when she asserts that a lack of such legislation has hurt personal privacy in the US, particularly given what is now known about the extent to which some security interests have pushed the limits of law enforcement and national security exceptions.

In summary, it seems reasonable to assert that current US data protection legislation has failed to achieve a satisfactory balance between the interests of the individual and those of security and commerce. Ironically, numerous consumer surveys have pointed to the negative commercial impact of privacy violations that have occurred in the name of security (Cobb, 2013; Cobb, 2014a; Cobb, 2014b). At the same time, there is plenty of evidence that few Americans are confident that their records will remain private and secure in the hands of commercial entities (Rainie, 2016). Sadly, more than four decades after Ware (1973) articulated a Code of Fair Information Practice for Americans "Ninety-one percent of [US] adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies" (Rainie, 2016).

Note: The contents of paper do not constitute legal advice and should not to be acted on as such. Furthermore, laws and case law constantly evolve so the information in this paper may no longer be current, or complete (some laws that have data privacy implications were not addressed herein, such as the Electronic Communications Privacy Act of 1986). Portions of this white paper were created as part of an essay assignment undertaken by the author during his studies for the *MSc in Security and Risk Management* in the Criminology Department of the University of Leicester in England. Any opinions expressed in this paper are those of the author and not his employer.

References

American Library Association (2015) *State Privacy Laws Regarding Library Records*. Available at: http://www.ala.org/advocacy/privacy/statelaws (accessed 21 December, 2015).

Baumer, D.L., Earp, J.B. and Poindexter, J.C., (2004) 'Internet privacy law: A comparison between the United States and the European Union' *Computers & Security* **23**(5): 400-412.

Bennett, C.J. (1992) *Regulating Privacy Data: Protection and Public Policy in Europe and the United States*, Ithaca, NY: Cornell University Press.

Bennett, C.J. (2011) 'In defense of privacy: the concept and the regime' *Surveillance & Society*, **8** (4): 485-496.

Bignami, F. (2007) 'European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining' *Boston College Law Review* **48**(609). Available at http://lawdigitalcommons.bc.edu/bclr/vol48/iss3/3 (accessed 1 December 2015).

Bloom, R.M. and Dunn, W. J. (2006) 'The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment' *William & Mary Bill of Rights Journal* **15**: 147-202.

Brown, I. (2012) 'Government Access to Private-Sector Data in the United Kingdom', *International Data Privacy Law* **2**(4): 230-238.

Cable Communications Policy Act of 1984, 47 U.S.C. § 551. Available at: https://www.law.cornell.edu/uscode/text/47/551 (accessed 1 December 2015).

Cate, F.H. (1995) 'The EU Data Protection Directive, information privacy, and the public interest', *Iowa Law Review* **80**(3): 431-443.

Cate, F.H., Dempsey, J.X. and Rubinstein, I.S. (2012) 'Systematic government access to private-sector data' *International Data Privacy Law* **2**(4): 195-199.

Chemerinsky, E. (2009) 'Civil liberties and the war terror: seven years after 9/11 history repeating: due process, torture and privacy during the war on terror' *SMU Law Review* **62**(1): 3-15.

Chemerinsky, E. (2014) *The Case Against the Supreme Court*, New York: Penguin.

Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6502. Available at: https://www.law.cornell.edu/uscode/text/15/6502 (accessed 1 December 2015).

Cobb, S. (2002) *Privacy for Business: Web Sites and Email*, Saint Augustine, FL: Dreva Hill. Available at http://privacyforbusiness.com/agreement.html (accessed 2 December 2015).

Cobb, S. (2003) 'The Privacy-Security Dialogue' *Privacy Officers Advisor* **3**(5): 8-10.

Cobb, S. (2013) 'Survey says 77% of Americans reject NSA mass electronic surveillance, of Americans' *We Live Security*, 29th October. Available at http://www.welivesecurity.com/2013/10/29/survey-says-77-of-americans-reject-nsa-mass-electronic-surveillance-of-americans/ (accessed 20 February 2016).

Cobb, S. (2014a) 'New Harris poll shows NSA revelations impact online shopping, banking, and more' *We Live Security*, 2nd April. Available at http://www.welivesecurity.com/2014/04/02/harris-poll-nsa-revelations-impact-online-shopping-banking/ (accessed 20 February 2016).

Cobb, S. (2014b) 'N Could latest NSA revelations further impact online behavior, denting the economy?' *We Live Security*, 8th July. Available at http://www.welivesecurity.com/2014/07/08/nsa-revelations-tor-linux-90-percent/ (accessed 20 February 2016).

COE (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37 (accessed 13 November 2015)

COE-FRA (2014) *Council of Europe European Union Agency for Fundamental Rights Handbook on European data protection law*. Available at http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (accessed 7 December 2015).

Coplan, J. (2015) '5 states with the most Fortune 500 companies' *Fortune*, 30th June. Available at http://fortune.com/2015/06/30/states-most-fortune-500/ (accessed 12 December 2015).

Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721. Available at: https://www.law.cornell.edu/uscode/text/50/1881a (accessed 1 December 2015).

Dvorak, K (2016) 'Medical research institute to pay $3.9M in HIPAA settlement: Feinstein Institute for Medical Research represents OCR's second target in a week' *FierceHealthIT*, 18th March, http://www.fiercehealthit.com/story/medical-research-institute-pay-39m-hipaa-settlement/2016-03-18 (accessed 11 April 2016).

EPIC (2015) *EPIC v. FBI - Stingray / Cell Site Simulator*, https://epic.org/foia/fbi/stingray/ (accessed 1 December 2015).

EPIC (2016) *Video Privacy Protection Act*, https://epic.org/privacy/vppa/ (accessed 12 April 2016).

Etzioni, A. (2015) 'NSA: National security vs. individual rights' *Intelligence and National Security* **30**(1): 100-136.

EU (1995) '95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data' *Official Journal of the EC*, **23**(6).

Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006). Available at: https://www.law.cornell.edu/uscode/text/15/1681 (accessed 1 December 2015).

Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232 (2006). Available at: https://www.law.cornell.edu/uscode/text/20/1232g (accessed 1 December 2015).

Farivar, C. (2015) 'California cops, want to use a stingray? Get a warrant, governor says' *ArsTechnica.com*, 8th October, http://arstechnica.com/tech-policy/2015/10/california-governor-signs-new-law-mandating-warrant-for-stingray-use/ (accessed 19 December 2015).

Federal Trade Commission Act of 1914, 15 U.S. Code § 41. Available at https://www.law.cornell.edu/uscode/text/15/41 (accessed 12 November 2015).

FTC (2002) *FTC v. Eli Lilly,* https://www.ftc.gov/enforcement/cases-proceedings/012-3214/eli-lilly-company-matter (accessed 15 December, 2015).

FTC (2015a) *LifeLock to Pay $100 Million to Consumers to Settle FTC Charges it Violated 2010 Order*, https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated (accessed 24 December 2015).

FTC (2015b) *FTC v. Wyndham,* https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation (accessed 15 December 2015).

GAO (2015) *Federal Agencies Need to Better Protect Sensitive Data*, GAO-16-194T, http://www.gao.gov/products/GAO-16-194T (accessed 1 December, 2015).

Gellman, R. (2014) 'Willis Ware's Lasting Contribution to Privacy: Fair Information Practices', *IEEE Security & Privacy* **12**(4): 51-54.

Goede (2014) 'The Politics of Privacy in the Age of Preemptive Security' *International Political Sociology* **8**: 100–118.

Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6803 (2012). Available at: https://www.law.cornell.edu/uscode/text/15/6803 (accessed 1 December 2015).

Greenwald, G. (2013) 'The Crux of the NSA Story in One Phrase: Collect It All' *The Guardian*, 15th July. Available at http://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all (accessed 12 December 2015).

Gutierrez, G. (2014) 'Imbalance of Security & Privacy: What the Snowden Revelations Contribute to the Data Mining Debate' *Intell. Prop. L. Bull*. **19**(2): 161-181.

Habermas, J. and Rehg, W. (2001) 'Constitutional democracy: a paradoxical union of contradictory principles?' in J. Habermas and W. Rehg

(eds) *Deliberative Democracy: Essays on Reason and Politics,* Cambridge, MA: MIT Press, 766-781.

Halpert, J. and White, S. (2013) 'Congress makes compliance with the confusing Video Privacy Protection Act easier' *DLA Piper*. Available at https://www.dlapiper.com/en/us/insights/publications/2013/01/congress-makes-compliance-with-the-confusing-vid__/ (accessed 1 December 2015).

Health Insurance Portability and Accountability Act of 1996, 29 U.S.C. § 1181 (2006 & Supp. V 2011). Available at: https://www.law.cornell.edu/uscode/text/29/1181 (accessed 1 December 2015).

ICO (2015) *Key definitions of the Data Protection Act* https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/ (accessed 2 December 2015).

Kirkham, C. (2016) 'California cranks out new businesses and jobs despite criticism' *LA Times*, 2nd January. Available at http://www.latimes.com/business/la-fi-business-climate-20160102-story.html (accessed 2 January 2016).

Koops, B. (2014) 'The trouble with European data protection law', *International Data Privacy Law* **4**(4): 250-261.

Loten, A (2015) 'OPM Data Breach Tops List of 'Federal Fumbles'' *Wall Street Journal*, 1st December. Available at http://blogs.wsj.com/cio/2015/12/01/opm-data-breach-tops-list-of-federal-fumbles/ (accessed 2 January 2016).

Lyon, D. (2015) 'The Snowden stakes: challenges for understanding surveillance today' *Surveillance & Society* **13**(2): 139-152.

Mitsilegas, V. (2015) 'The transformation of privacy in an era of pre-emptive surveillance' *Tilburg Law Review* **20**(1): 35-57.

Murphy, E., 2013 'The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions. *Michigan Law Review* **111**(4): 485-546.

National Conference of State Legislatures (2015a) *Privacy Protections in State Constitutions,* http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx (accessed 12 December 2015).

National Conference of State Legislatures (2015b) *Security Breach Notification Laws*, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (accessed 12 December 2015).

National Conference of State Legislatures (2015c) *State Laws Related to Internet Privacy*, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (accessed 12 December 2015).

Newland, E. (2015) 'Executive Orders in Court' *Yale LJ*, **124**: 2026-2189.

Nixon, R. M. (1974) *Radio Address About the American Right of Privacy*. Available at: http://www.presidency.ucsb.edu/ws/?pid=4364 (accessed 1 December 2015).

OECD (2013) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 10 November 2015).

Ombres, D. (2015) 'NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History, Constitutional Basis, and the Efforts at Reform' *Seton Hall Legis. J.* **39**: 27-58.

Owsley, B.L (2014) 'Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions. *Hastings LJ*, **66**: 183-232.

Pell, S. and Soghoian, C. (2015) 'A Lot More than a Pen Register, and Less than a Wiretap' *Yale Journal of Law and Technology*, **16**: 134-171. Available at http://pdfserver.amlaw.com/nlj/SSRN-id2458076.pdf (accessed 1 December 2015).

Peltz-Steele, R. J. (2015) 'The Pond Betwixt: Differences in the US-EU Data Protection/Safe Harbor Negotiation' *Journal of Internet Law*, **19** (1): 1,15-30.

PRC (2015) 'Chronology of Data Breaches Security Breaches 2005 – Present' *Privacy Rights Clearinghouse* http://www.privacyrights.org/data-breach (accessed 19 December 2015).

Privacy Act of 1974, 5 U.S.C. § 552a (2006 & Supp. V 2011). Available at: https://www.law.cornell.edu/uscode/text/5/552a (accessed 1 December 2015).

Rainie, L. (2016) 'The state of privacy in America: What we learned' *PewResearchCenter*, 20th January. Available at http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/ (accessed 20 February 2016).

Regan, P.M. (1984) 'Personal information policies in the United States and Britain: The dilemma of implementation considerations' *Journal of Public Policy*, **4**(01): 19-38.

Reidenberg, J.R. (2014) 'The data surveillance state in the United States and Europe', *Wake Forest Law Review,* **49**(2): 583-608 .

Right to Financial Privacy Act of 1978, 12 U.S.C. § 3408 (2006). Available at: https://www.law.cornell.edu/uscode/text/12/3408 (accessed 1 December 2015).

Robinson, J. (2014) The Snowden Disconnect: When the Ends Justify the Means' *SSRN*. Available at: http://dx.doi.org/10.2139/ssrn.2427412 (accessed 13 December 2015).

SCOTUS (1928) *Olmstead v. United States*, 277 U.S. 438. Available at https://www.law.cornell.edu/supremecourt/text/277/438 (accessed 25 November 2015).

SCOTUS (1939) *United States v. Miller*, 307 U.S. 174. Available at https://www.law.cornell.edu/supremecourt/text/307/174 (accessed 29 November 2015).

SCOTUS (1976) *Fisher v. United States*, 425 U.S. 391. Available at http://caselaw.findlaw.com/us-supreme-court/425/391.html (accessed 29 November 2015).

Serwin, A. (2011) 'The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices' *San Diego L. Rev.* **48:** 809-856.

Serwin, A. (2015) 'The FTC v. Wyndham Reexamined – A True Test of the Contours of Unfairness' *The Lares Institute Blog*, 28th September, http://www.laresinstitute.com/archives/4631 (accessed 14 November 2015).

Simard, A and Griffin, S. (2014) 'Proactive Monitoring: Lack of Employee Oversight Leads to the Certification of the first Privacy Class Action based on the novel tort of "intrusion upon seclusion"' Canadian Class Actions Monitor, 23rd June, http://www.canadianclassactionsmonitor.com/2014/06/proactive-monitoring-lack-of-employee-oversight-leads-to-the-certification-of-the-first-privacy-class-action-based-on-the-novel-tort-of-intrusion-upon-seclusion/ (accessed 13 November 2015).

Snell, E. (2015) 'Lessons Learned From the 2015 OCR HIPAA Settlements' *HealthITSecurity.com* 18th December, http://healthitsecurity.com/news/lessons-learned-from-the-2015-ocr-hipaa-settlements (accessed 24 December 2015).

Solove, D.J. and Hartzog, W. (2014) 'The FTC and the New Common Law of Privacy' *Columbia law review,* **114**(3): 583-676.

Stevens, G. (2014) *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, Congressional Research Service http://fas.org/sgp/crs/misc/R43723.pdf (accessed 1 December 2015).

Swire, P. P. and Ahmad, K. (2012a) *Foundations of Information Privacy and Data Protections*, Portsmouth, NH: International Association of Privacy Professionals.

Swire, P. P. and Ahmad, K. (2012b) *U.S. Private-sector Privacy*, Portsmouth, NH: International Association of Privacy Professionals.

Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. § 1039 (2006). Available at: https://www.law.cornell.edu/uscode/text/18/1039 (accessed 1 December 2015).

US Const. amend. IV. https://www.law.cornell.edu/constitution/fourth_amendment (accessed 15 December 2015).

Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2006). Available at:

https://www.law.cornell.edu/uscode/text/18/2710 (accessed 1 December 2015).

Waldo, J., Lin, H. and Millett, L.I. (2007) *Engaging privacy and information technology in a digital age*. Washington, DC, USA: National Academies Press.

Ware, W. H. (1973) *Records, Computers, and the Rights of Citizens*, RAND. Available at https://www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf (accessed 29 November, 2015).