INFORMATION SECURITY & PRIVACY NEWS

A Publication of the Information Security Committee
ABA Section of Science & Technology Law

WINTER 2014 VOLUME 5 ISSUE 1

Managing Information in Digital Form

By Patrice A. Lyons

Much energy has been spent over the past few years on what is often called Software Defined Networking (SDN). In some efforts there appears to be a distinction drawn with respect to certain basic terminology: namely, the meaning of the concepts “program” and “data;” and how they may apply in the context of SDN. A careful examination of these basic building blocks in the context of an SDN environment leads to the following conclusion -- it is not really helpful to draw a distinction between what is called “data transport” and what is called “data management.” The rationale is as follows: There is a need for transparency and interoperability across different information systems and the many discrete elements of which they may be comprised. *Read more*

Privacy: Individual and Group Rights

By Martha A. Chemas

Are privacy rights group rights or individual rights or some combination thereof? In what follows I will broadly survey the philosophical implications of: Supreme Court caselaw in three important privacy cases, the privacy related laws one is expected to master to earn the accreditation “CIPP” and Article 22 of the UN Convention on Persons with Disabilities, in an effort to shed some light on our question. The now ubiquitous dialogue about privacy could begin with the acknowledgement that instead of a coherent and methodical jurisprudential regime, what currently exists is a patchwork of laws and decisions developed piecemeal, throughout the course of addressing practical concerns. This observation lead me to identify a mostly unaddressed binary *Read more*

Seizing Electronic Evidence from Cloud Computing Environments

By Josiah Dykstra

Crime committed using cloud computing resources and against cloud infrastructures is inevitable. In early 2011, Sony was the victim of an online data breach that took down the PlayStation Network. In a widely cited report, Bloomberg News reported that the intruder used Amazon’s public cloud to commit the crime. The report also stated that the FBI was investigating the crime, but that neither Amazon nor the FBI would comment on whether the former had been served a search warrant or subpoena. No further information about the case has been made public. This is the first public case of a cloud-related crime, though many more are bound to emerge soon. Companies are embracing cloud technology to offload some of the cost, upkeep, and *Read more*

2013 (2H) Information Law Updates: Cases, Statutes, and Standards

By Thomas Shaw

In the second half of 2013 and the end of the first half, there have been many developments in U.S. and international information security and privacy statutes, cases and standards. This includes international and U.S. state and federal laws and regulations that have been passed or are coming into force. It also involves civil and criminal cases and enforcements actions brought by regulators. And it encompasses the new standards, guidelines and legal ethics opinions in this area. But it leaves out cases on recurring themes and it does not attempt to track legislation that has not been passed. To briefly summarize the major developments in this area of law and practice, each significant development is presented with a brief analysis after it. *Read more*

Managing Data in Digital Form

By Patrice A. Lyons

Much energy has been spent over the past few years on what is often called Software Defined Networking (SDN). In some efforts there appears to be a distinction drawn with respect to certain basic terminology: namely, the meaning of the concepts "program" and "data;" and how they may apply in the context of SDN. A careful examination of these basic building blocks in the context of an SDN environment leads to the following conclusion -- it is not really helpful to draw a distinction between what is called "data transport" and what is called "data management." The rationale is as follows: There is a need for transparency and interoperability across different information systems and the many discrete elements of which they may be comprised (for use case, see Exhibit A below). Linguistic definitions that limit one's conceptual horizons might prove to be insurmountable barriers that serve to inhibit progress in such a dynamic technical discipline.

In the late 1980's at Corporation for National Research Initiatives in Reston, Virginia, known as CNRI, Robert Kahn and Vinton Cerf were involved in many projects relating to infrastructure research and development including various technology for managing information represented in digital form and the deployment of this technology in the Internet. A CNRI project called Knowledge Robots (or simply Knowbots) focused on the design and deployment of mobile programs in the Internet to perform tasks on behalf of users. Such a system was actually built and demonstrated. Various sites in the Internet were configured as Knowbot Service Stations that permitted software controlled intermediation between the network environment and specific collections of information or other digital resources. This mobile programming technology provided a type of software defined operating capability that was organized around the management of dynamic units of information that were identifiable within a given network environment. A part of this work was later separated out and went on to become what is known as the Digital Object (DO) Architecture (overview of the DO Architecture is available at

http://www.cnri.reston.va.us/papers/OverviewDigitalObjectArchitecture.pdf).

A key component of the DO Architecture is the unique persistent identification of information represented as or converted to a machine independent data structure consisting of one or more elements in digital form; these structures are known as digital objects or, more abstractly, digital entities. The term digital entity is a key conceptual element in a new international standard (ITU-T X.1255 Recommendation) approved at an International Telecommunication Union (ITU) meeting in Geneva (ITU-T Study Group 17 (Security), August 26 to September 4, 2013; ITU announcement: http://newslog.itu.int/archives/137) that is focused on identity management information, but would apply more generally to many different types of information in digital form. The new Recommendation on "Framework for discovery for identity management information" is now available in English at

http://www.itu.int/rec/T-REC-X.1255-201309-I, and will soon be released by ITU in the other official UN languages.

While compatible with today's Domain Name System (DNS) that is used to name specific machines in the Internet, where the names resolve to Internet Protocol (IP) addresses that identify ports on hardware components such as computers, a digital object has an associated handle, or more generically a digital object identifier, that resolves to state information about the object itself. This state information can be assigned by the creator of the object to include location information, authentication information, public keys (which are useful for validating individuals and systems, as well as other resources), and, more generally, the kinds of "stated operations" that may be applied to specific objects. Stated operations must be described in a deterministic way so that you (or in reality programs acting on your behalf) can actually use the information in a productive way.

Since a digital object consists simply of a sequence of bits, or a set of sequences of bits, with an associated unique persistent identifier, what is identified is the object itself, or parts thereof. This is sufficient to identify networks, services, documents, permissions information, transport instructions, chip designs, music, routers, or any other information represented as or converted to a machine independent data structure, as well as related information, usually referred to as metadata, such as who is authorized to access an object. In short, this technology applies to any information consisting of one or more elements expressed in digital form that is structured as a digital object.

Let's take routers as an example. While most individuals view a router as a piece of hardware with embedded software, sometimes called firmware, it may also be viewed, logically speaking, as a piece of executable software that happens to be running at any point in time on a piece of hardware. When a router is viewed as a piece of software, with its own associated unique persistent identifier, or in other words as a digital object that is independent of the hardware on which it is running, the router software can be moved from one piece of hardware to another (that is capable of running the software), without disrupting the logical organization of the system in which it is deployed. In this way the router becomes a kind of mobile program that may move from time to time depending on the task to be performed.

The technology for mobile programs also holds out the promise of enabling various SDN implementations not just to be deployed in the Internet or other computational environments, but also to permit the ongoing management of the information that is being made available in this new digital form of expression.

Coming back to the distinction between "data transport" and "data management" -- enabling access to perform stated operations on a digital object can apply to the ability to "transport" information in digital form as a type of operation invoked to carry out one or more management tasks for users, or, more likely, programs operating on their behalf. Other types of operations might include operations such as deposit, access, register, aggregate, verify or create identifier.

An important feature of an implementation of the DO Architecture is the capability of incorporating permissions information in metadata associated with the data being managed. For example, in a cloud computing environment, and here what is sometimes called "cloud computing" is viewed essentially as distributed computation services in the Internet, a large data center might manage the "stated operations" for many different customers. In addition to providing identifier and/or resolution services, the data center could deploy two other components of the DO Architecture: namely, the DO Repository (to store and access DOs, with security afforded by a public key infrastructure (or PKI)), or the DO Registry (which stores metadata about DOs and allows searching with PKI security). In a cloud computing service, the access conditions for operations that may be performed by the manager of a data center on a collection of information would often differ from the access conditions set by the individuals or organizations depositing their digital resources in such a center.

The technology that is the subject of the new Recommendation may also facilitate the deployment of what is sometimes called the "Internet of Things." A contribution to a book recently published by the American Bar Association's Business Law Section contains a chapter that addresses this subject (*see* R.E. Kahn and P.A. Lyons, "The Handle System and its Application to RFID and the Internet of Things," RFIDs, Near-Field Communications, and Mobile Payments, Ch. 13, p. 257, S.J. Hughes, Editor, ABA Cyberspace Law Committee, Business Law Sec. (2013)).

Combined instances of these three components may be implemented together as a general information management resource; and here, the notion of a DO Repository is not the same as a database. It is rather a technology independent interface into one or more databases or other collections of information. This interface is enabled using the unique persistent identifier for the repository -- itself represented as a digital object, as well as each unit of information in the collection of information that is also represented as a digital object having an associated unique persistent identifier.

This technology has been deployed in the Internet over the past twenty years. It is in widespread use in the publishing industry where the International DOI Foundation (http://www.doi.org) was established to manage its implementation of the DO Architecture, called the DOI System, that is based on, in particular, CNRI's Handle System technology and reference software (http://www.handle.net). Recently interest has been expressed in implementing this technology to manage very large collections of information in such areas as health care or sensor nets.

A final thought on the overall SDN terminology: several years ago, a highly respected Computer Scientist at Carnegie Mellon University, Allen Newell, who has since passed away, became interested in computer science concepts as they were applied in the intellectual property area. He wrote an article which is still available in the Internet: "The Models are Broken, The Models are Broken!" in which he expressed concern about what appeared to be a distinction being made between the term "computer program" (or, more generally, "software") and the term "data." It was his firm view that: "…. the boundary between data and program – that is, what is data and what is procedure – is very fluid. In

fact, … there is no principled distinction in terms of form or representation of which is which. What counts is the total body of knowledge represented somehow in the assembled symbolic expressions" (47 University of Pittsburgh Law Review 1023, 1031 (1986)).

Applying this observation to ongoing efforts on SDN: as the SDN work is in its early stages there is still time to step back a bit and rethink the basic terminology as applied to the technology under development. A better approach would be to explore the implementation of these elements structured as unique persistently identifiable digital objects. If one focuses on the actual technical characteristics of an SDN environment and views the elements as representing assembled symbolic logic expressed in digital form and structured as digital objects, it may be apparent that this is similar in many ways to the approach taken by CNRI in its original work on mobile programs.

Development efforts could then turn to reaching some initial understandings about what access to perform stated operations may be contemplated in an SDN environment, as well as metadata schema and type registries to enable discovery of relevant information. If done thoughtfully, such understandings could both advance the technology and provide a flexible way to transport and otherwise manage not just information and other resources in digital form for purposes of SDN, but to provide more flexibility and transparency across various information systems, and the elements thereof, in distributed computational environments.

*As General Counsel to Corporation for National Research Initiatives (CNRI), **Patrice Lyons** has been involved in the analysis of a wide range of legal and regulatory issues relating to the development of the Internet, including work on the establishment of the Internet Society and the provision of legal support to the Internet Engineering Task Force (IETF) Secretariat. Ms. Lyons has participated in the development of CNRI's Digital Object Architecture, in particular, the Handle System component, so that it may be made available to interested parties around the world. She has also provided advice and guidance to CNRI with respect to a variety of trademark, patent, copyright and other general legal matters.*

Ms. Lyons' interest in the application of copyright and related bodies of law to new technical developments began upon graduation from Georgetown University Law Center (J.D.1969), when she attended Columbia University Law School (1969-70) as the Burton Memorial Fellow in copyright and communications studies. While a legal officer in the Copyright Division of UNESCO (Paris, France; 1971-76), she participated in the preparation of the Convention relating to the Distribution of Programme-Carrying Signals transmitted by space satellite; as a Senior Attorney in the Office of General Counsel of the U.S. Copyright Office, Library of Congress (1976-87), she worked on the drafting of various regulations, including the cable licensing system adopted by the U.S. Congress in 1976, and contributed to the preparation of the Semiconductor Chip Protection Act of 1984. Ms. Lyons was a Partner in the communications law firm of Haley, Bader & Potts (1987-90), and is currently in practice in Washington, D.C. at Law Offices of Patrice Lyons, Chartered. She is a member of the bars of New York State, District of Columbia and U.S. Supreme Court.

Privacy: Individual and Group Rights

By Martha A. Chemas

Are privacy rights group rights or individual rights or some combination thereof? In what follows I will broadly survey the philosophical implications of: Supreme Court caselaw in three important privacy cases, the privacy related laws one is expected to master to earn the accreditation "CIPP" and Article 22 of the UN Convention on Persons with Disabilities, in an effort to shed some light on our question.

Introduction

The now ubiquitous dialogue about privacy could begin with the acknowledgement that instead of a coherent and methodical jurisprudential regime, what currently exists is a patchwork of laws and decisions developed piecemeal, throughout the course of addressing practical concerns. This observation lead me to identify a mostly unaddressed binary in privacy; there is distinction between group rights and individual rights with regard to the existing body of work in this area, and in order to arrive at a more coherent jurisprudence, it may be helpful to compare and contrast how the group based rights and the individual based rights operate to protect privacy.

To try and learn more about how we have been conceiving the idea of privacy, from within this lens of the group versus the individual binary, I want to examine three basic areas to see what light they can shed on our method. First, let's review what is denoted by "group rights" and "individual rights."

Group Rights v Individual Rights

Let us refresh our recollection of the defining characteristics of group or individual rights:

Group rights are implicated when the "Individual is part of a group with fixed characteristics not unique to single individuals nor the result of individual achievement.[1]" **"**Individual rights must always be balanced against the requirements of the group.[2]" Group rights related theories are an important component of political philosophy: "Justice requires removing or compensating for undeserved

[1]See http://heinonline.org/HOL/LandingPage?handle=hein.journals/hurq13&div=26&id=&page= accessed 11.26.13.
[2]See http://www.jstor.org/discover/10.2307/761878?uid=3739832&uid=2&uid=4&uid=3739256&sid=21102967850997 accessed 11.26.13.

"morally arbitrary" disadvantages, particularly if these are "profound, pervasive and present from birth." "From The Rights of Minority Cultures," paraphrasing Rawls and Dworkin.[3]

Group and individual rights only make sense within this context of a dichotomy. Without group rights individual rights are meaningless and vice versa, and it is the balance of pressure of one against the other that gives the analysis of either coherence. If the rights of the group are defined by that which is immutable, shared by the group and devoid of any characteristic that pertains to merit, then it makes sense to ascribe to individual rights that which is necessarily not shared and wholly pertaining to what makes any individual unique. Any analysis of an individual based right is unquestionably related to the meritorious characteristics of the particulars and these particulars can be facts as they relate to the specifics of a matter, or characteristics as they relate to the individual. Choice, then, or lack thereof, has much to do with the analysis of whether a set of particulars can be analyzed through an individual or group lens.

Supreme Court Cases on Privacy

The right to privacy, it has been said, can be found in the penumbra of the First Amendment, as a sort of corollary of the right of association. But there is much more to privacy than just one Amendment.

The three cases I choose to help us further synthesize and contextualize the notion of individual rights versus group rights are *Griswold v Connecticut*[4], 381 US 479 (1965), *Soldal v. Cook County*[5], 506 US 56 (1992) and *US V Jones*[6], 132 S. Ct. 945 (2012). Let's take a look at them from the earliest case, in 1965 and follow through to 2012 to trace the logic of the court over this time frame. Also we will see that the court treats privacy as a procedural as well as substantive right.

In *Griswold v Connecticut*[7], the appellants, an executive director of Planned Parenthood in Connecticut, and its Medical Director, a licensed physician and professor at Yale, were arrested, convicted and fined pursuant to §§ 53-32 and 54-196 of the General Statutes of Connecticut (1958 rev.), for being accessories in the prevention of human conception. The appellants had prescribed contraceptives to their patients. The Appellate Division, and the Supreme Court of Errors confirmed the conviction. The Supreme Court begins its analysis by noting that it believes the appellants "have standing to raise the constitutional rights of the married people with whom they had a professional relationship" and goes on to say: "The rights of husband and wife, pressed here, are likely to be diluted or adversely affected unless those rights are considered in a suit involving those who have this kind of confidential relation to them." The majority finds that the fact pattern "concerns a relationship lying within the zone of

[3] See http://www.jstor.org/discover/10.2307/191782?uid=3739832&uid=2&uid=4&uid=3739256&sid=21102967850997 accessed 11.26.13.
[4] *Griswold v Connecticut*, 381 US 479 (1965).
[5] *Soldal v. Cook County*, 506 US 56 (1992).
[6] *US V Jones*, 132 S. Ct. 945 (2012).
[7] *Griswold v Connecticut*, 381 US 479 (1965).

privacy created by several fundamental constitutional guarantees," reasoning that the Due Process Clause of the Fourteenth Amendment, along with the First Amendment, the Third, Fourth and Fifth Amendment all operate to protect privacy, and as such, a law forbidding the use, rather than regulating the manufacture or sale of contraceptives is overbroad.

In *Soldal v. Cook County*[8], Soldal, the tenant of a trailer home in Cook County Illinois, brings a 42 U. S. C. § 1983[9] action alleging a violation of his rights under the Fourth and Fourteenth Amendment, after the employees of his landlord, without an eviction order, evicted Soldal from his trailer park by wrenching the sewer and water connections off the side of his trailer home. They also disconnected the phone, tore off the trailer's canopy and skirting, and hooked the entire home to a tractor. Cook County Sheriff's Department were present, to make sure Soldal did not offer resistance. The Supreme Court reversed[10] the District Court and Seventh Circuit Court holding[11] that removal of the Soldals' trailer did not constitute a seizure for purposes of the Fourth Amendment or a deprivation of due process for purposes of the Fourteenth, noting that the Fourth Amendment is implicated in civil contexts as well as in criminal contexts and that reasonableness is still the ultimate standard under the Fourth Amendment.

In *US v Jones*[12], the defendant, a suspected cocaine dealer, sought exclusion of all evidence obtained via a GPS tracking device that was placed on his vehicle without his consent. The United States Court of Appeals overturned[13] the lower court's conviction, on the grounds that the tracking device was a search that violated the defendant's expectation of privacy. Certiorari was granted in June of 2011[14], after which the Supreme Court held that installing a GPS tracking device on the defendant's vehicle and using the device to monitor the vehicle's movements constituted a search under the Fourth Amendment[15]. The matter was remanded to the DC court, where the District Court judge allowed the use of cell phone location data pursuant to the Stored Communications Act[16]. After a mistrial Jones eventually accepted a plea.

The remand is particularly interesting for our purposes because the data admitted via the Stored Communications Act had the net effect of supplying substantially similar, if not the same, data about Jones that the GPS device did, via the defendant's custom of carrying his cell phone, rather than via his habit of riding in his car.

---

[8] *Soldal v. Cook County*, 506 US 56 (1992).
[9] See http://www.law.cornell.edu/uscode/text/42/1983 accessed 11.26.13.
[10] *Soldal v. Cook County*, 506 US 56 (1992).
[11] *Soldal v Cook County,* 942 F.2d 1073 (1991).
[12] *US v Jones*, 132 S. Ct. 945 (2012).
[13] *US v Maynard*, 615 F.3d 544 (D.C. Cir. 2010).
[14] *US v Jones*, 131 S. Ct. 3064 (2011).
[15] *US v. Jones*, 132 S. Ct. 945 (2012).
[16] See https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2005cr0386-658 accessed 11.26.13.

In the earliest case[17] we see the court reasoning that privacy is protected at various places by the Bill of Rights as well as via the Due Process Clause of the Fourteenth Amendment. Generally speaking the operation of these rights is via a theory of individual rights as well as group rights. The right of free expression guaranteed by the First Amendment has both procedural and substantive components, but either is related to the particulars, rather than the immutable characteristics of the individual, as it is the latter part of the First Amendment that addresses a group right, via the Establishment Clause. The Third Amendment in its prohibition against the quartering of soldiers "in any house" may be best understood as a privacy right rooted in group rights, as surely the individual who might object to such a thing would have had little choice in determining whether it is peacetime or wartime. The Fourth Amendment, as viewed by the Griswold Court, is also a procedural right and clearly pertains to the rights of the individual. The Fifth Amendment right against self-incrimination implicates both group and individual rights; the Majority in Griswold states that it: "create(s) a zone of privacy which government may not force him to surrender to his detriment."

As we follow through to *Soldal*[18], the focus of the inquiry is on the Fourth and Fourteenth Amendment, as this is a case that turns on the notion of state action with regard to an individual's private property. Thus procedural and substantive rights are implicated, the Third and Fifth Amendments are not mentioned, as they do not have applicability with regard to the particular fact pattern. The rights here are exclusively individual based rights, the immutable characteristics of the appellant do not enter the court's reasoning.

The *Jones*[19] court also focuses on individual based rights, as the fact pattern also gives rise to an inquiry about whether a particular individual's expectation of privacy was implicated.

CIPP Rules

Bearing in mind the decisions we just addressed, let's now turn our attention to rulemaking within the sphere of privacy. To begin this research, I Googled: "Privacy accreditation legal" without quotes and was rewarded with results, the more interesting of which were those for the CIPP certification. CIPP is an abbreviation for "Certified Information Privacy Professional," it is a professional certification that, according to its website: "demonstrates a strong foundation in U.S. privacy laws and regulations and understanding of the legal requirements for the responsible transfer of sensitive personal data to/from the United States, the European Union and other jurisdiction." One does not have to be an attorney to be a CIPP. To master the subject matter tested on the CIPP exam one must demonstrate knowledge of:

- The U.S. legal system: definitions, sources of law and sectoral model for privacy enforcement
- U.S. federal laws for protection of personal data: FCRA and FACTA, HIPAA, GLBA, COPPA and DPPA

[17] *Griswold v Connecticut*, 381 US 479 (1965).
[18] *Soldal v. Cook County*, 506 US 56 (1992).
[19] *US V Jones*, 132 S. Ct. 945 (2012).

- U.S. federal regulation of marketing practices: TSR, DNC, CAN-SPAM, TCPA and JFPA
- U.S. state data breach notification and select state laws
- Regulation of privacy in the U.S. workplace: FCRA, EPP, ADA and ECPA plus best practices for privacy and background screening, employee testing, workplace monitoring, employee investigation and termination of employment"[20]

These are fairly broad domains within American law, and in order to keep this to approximately two-thousand words I can really only address some broad strokes, but if this gets the rest of us thinking about the bigger issues in privacy, that may help as we, collectively, as legal professionals, think about how to address some of the logistical hurdles of our time, with respect to the technology attorneys use to communicate all the time, and how this may or may not have an impact on the institution of attorney-client privilege.

Okay, the first one says:

"The U.S. legal system: definitions, sources of law and sectoral model for privacy enforcement"

Let us then acknowledge that any principles we derive from this thought experiment will be distinctively American in flavor, and, as we are increasingly dealing with a global approach to law, this is of particular significance because in the highest ranks of the cyberdefense arena, what is sought is an international framework by which to approach cybersecurity. Also let me assert that cybersecurity and privacy are two concepts that are intertwined; one cannot be considered without considering the other and to the extent that I am going to opine on this, it should be acknowledged early on that my training and context are American.

The second thing we get from looking at this list is that regulations that address this issue exist in the federal domain, thus there may be significant issues in the area of preemption to come.

Third, state breach notification laws exist. Fourth: Marketing and the workplace have received extra and special attention from legislators.

(For The Record: The word "privacy" does not appear in the index of my copy of the Uniform Commercial Code.)

Are these various pieces of legislation concerned with addressing the rights of the group or that of the individual? The federal laws operate to protect *both*. For example HIPAA, in protecting the privacy of minors aged 12-18 protects the child as an individual, with her own specific data, but it also is protecting her because she is a minor, which is an immutable characteristic not marked by choice. This argument may be carried to the other pieces of legislation, in some instances, as well.

[20] From https://www.privacyassociation.org/certification/cipp_certification_programs accessed 11.26.13.

Article 22 of the UN Convention on Persons with Disabilities

Finally, and briefly, let's take a look toward the international sphere. Finding the Convention on Persons with Disabilities[21] we see a group rights related approach to the protection of privacy:

Article 22 - Respect for Privacy

1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.

2. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others.[22]

This legislation, taken at its plain meaning exists to further a group right related set of concerns.

Questions Raised

Are privacy related rights group rights or are they individual based rights? How does a theory of either operate to protect privacy?

Conclusions

As we have seen from our broad strokes survey, privacy is a right rooted in both group rights and in individual rights related theories. Existing caselaw has examined the right in light of the multifaceted protection offered to it by the US Constitution's Bill of Rights as well as the Fourteenth Amendment, and both from the context of privacy being a procedural as well as a substantive right. Existing legislation approaches the right via group or individual rights related language or both. Thus, the deprivation of privacy is the deprivation of a substantive and procedural right of an individual, as well as of a group.

Martha C. Chemas, *Esq. is graduate of the City University of New York School of Law. She enjoys teaching, writing, research and the arts.*

[21] Accessed via: http://www.un.org/disabilities/convention/conventionfull.shtml on 11.26.13.
[22] See fn 21.

Seizing Electronic Evidence from Cloud Computing Environments

By Josiah Dykstra

Crime committed using cloud computing resources and against cloud infrastructures is inevitable. In early 2011, Sony was the victim of an online data breach that took down the PlayStation Network. In a widely cited report, Bloomberg News reported that the intruder used Amazon's public cloud to commit the crime.[23] *The report also stated that the FBI was investigating the crime, but that neither Amazon nor the FBI would comment on whether the former had been served a search warrant or subpoena. No further information about the case has been made public. This is the first public case of a cloud-related crime, though many more are bound to emerge soon.*

Companies are embracing cloud technology to offload some of the cost, upkeep, and growth of equipment that they would otherwise have purchased themselves. Cloud infrastructure offers an attractive prize for hackers, with exceptional bandwidth, storage and computing power, and a consolidated repository of data. While many people have lamented how users of the cloud and their data are protected, few of these discussions have considered the difficulty of responding to and prosecuting security breaches, including forensics and criminal prosecution.

Cloud computing introduces new and significant challenges in prosecuting cloud-based crimes that differ from traditional electronic evidence and electronic crime. The very attributes that make cloud computing attractive can be at odds with forensic and legal goals. For example, the cloud offers location independence so that data are available from anywhere, even though location may determine jurisdiction. Another example is the rapid self-creation and destruction of cloud resources, a powerful feature for customers, but a severe challenge for evidence preservation.

This article discusses technical details to consider when authoring a search warrant to seizure data from cloud computing related to the prosecution of cloud-based crimes. We previously explored the legal problems in the United States for electronic discovery and digital forensics arising from cloud computing as an infrastructure service and explained how cloud computing challenges the process and product of electronic discovery[24]. We approach the problem from a computer science perspective and with a background in digital forensics. This technical perspective is intended to aid legal practitioners with prosecuting cloud crimes.

---

[23] Galante, J., Kharif, O., & Alpeyev, P. (2011). Sony Network Breach Shows Amazon Cloud's Appeal for Hackers. *Bloomberg*. Retrieved November 2, 2011, from http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html

[24] Dykstra, J. and D. Riehl, "Forensic Collection of Electronic Evidence from Infrastructure-As-A-Service Cloud Computing," In Richmond Journal of Law and Technology, Volume 19, Issue 1, 2012.

We use a hypothetical case study of child pornography being hosted in the cloud to illustrate the difficulty in acquiring evidence for cloud-related crimes. While fictional, it describes a common computer crime where the cloud is an accessory to a crime. For the first time we present a sample search warrant affidavit that could be used in this case study. This provides an example and sample language for agents and prosecutors who will soon need to obtain a warrant authorizing the search and seizure of data from cloud computing environments.

Before looking at elements of a search warrant for cloud evidence, we provide some context and background about cloud computing and related work.

Cloud Computing

Let us being by defining the scope of our discussion. It would be easy to let a discussion on cloud computing grow to encompass all Internet-enabled services as "cloud computing." There are good reasons for discussing forensic investigations of Facebook and Twitter specifically because those services are involved in many cases, but we will take a more formal definition. One often-cited definition of cloud computing comes from the National Institute of Standards and Technology (NIST),[25] which reads in part:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

"Cloud" is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. Telephone networks and the Internet are examples of clouds. Cloud computing, however, is concerned with providing customers with raw remote computing resources such as computation or data storage, and the ability to provision those resources themselves.

There are many providers of cloud services, and even those that provide similar services have proprietary implementations. Amazon Web Services (AWS) is one example of a cloud service provider. AWS provides a variety of infrastructure as a service (IaaS) cloud services. The Elastic Compute Cloud (EC2) is a platform where customers can purchase computing power in the form of a computer connected to the Internet that the customer can control. The Simple Storage Service (S3) is a cloud storage offering, essentially acting like a large disk drive accessible from the Internet. Other examples of cloud service providers are Microsoft Azure, Salesforce, and Google AppEngine.

For the purposes of our discussion about seizing evidence, we focus on gathering evidence from IaaS cloud providers. Online services, including social networking sites and web-based email, inherently

[25] Mell, P. & Grance, T. (2011, September). The NIST Definition of Cloud Computing. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

have different data of interest in e-discovery. Technical and legal experts have already analyzed many issues related to e-discovery of these services, including the publication of real subpoenas and search warrants. Concentrating on IaaS cloud services, we will take as broad a view as possible. However, remember that each provider may implement their cloud services in a proprietary manner that may influence the forensic data available, how those data are collected, and who has access to the data.

Related Work

We are unaware of any published template for writing a search warrant for cloud data. In 2006, a California attorney published an article titled "Search Warrant Language for Cellular Phones," describing how to obtain data from cell providers.[26] Several law enforcement manuals, which describe what data are available to law enforcement and how to request them, for webmail and social networking websites have leaked online. These may hint at similar data available for cloud services. Several search warrants have appeared in the press for services like Facebook[27] and Gmail.[28] The Department of Justice Search and Seizure Manual[29] includes sample subpoenas, orders, and warrants which we used for guidance, but none of these were for cloud data.

Stephen Wolthusen highlighted a number of research challenges for forensic discovery in distributed environments.[30] While he enumerated some of the legal challenges, he did not analyze the applicability of existing laws. Another study looked more closely at UK-specific issues.[31]

Other authors have taken a careful look at privacy related to cloud computing, the most common topic of law review articles related to cloud computing. Stylianou studied changes in the privacy terms of cloud services, and found that more private information was being surrendered to third parties but that companies were treating that data with more respect.[32] Barnhill explained that court decisions extend no reasonable expectation of privacy in emails stored with third.[33] Couillard wrote, "users

---

[26] Morgester, R. (2006). Search Warrant Language for Cellular Phones. *Cyber Crime Newsletter*. Retrieved from http://www.olemiss.edu/depts/ncjrl/pdf/May-June%202006%20Final%20Copy.pdf.

[27] "You Look Like Obama": FBI Seeks Facebook Records for Person of Interest in Mosque Arson (2011, April 8). *Willamette Week*. Retrieved from http://www.wweek.com/portland/blog-26890-you_look_like_obama_fbi_seeks_facebook_records_for.html.

[28] Van Horn, C. (2009, May 30). Chris Coleman documents and search warrants. Retrieved from http://www.examiner.com/article/chris-coleman-documents-and-search-warrants.

[29] U.S. Department of Justice (2009). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Retrieved from http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

[30] Wolthusen, Stephen (2009). Overcast: Forensic Discovery in Cloud Environments. *Fifth International Conference on IT Security, Incident Management, and IT Forensics*, 3-9.

[31] Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigations of cloud computing systems. *Network Security*, 4-10.

[32] Stylianou, K. K. (2010). An Evolutionary Study of Cloud Computing Services Privacy Terms. *27 John Marshall Journal of Computer & Information Law*, 593-612.

[33] Barnhill, D. S. (2010). Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless. *25 Berkeley Technology Law Journal*, 621-671.

expect their information to be treated the same on this virtual cloud as it would be if it were stored on their computer, phone, or iPod."[34]

Obtaining Forensic Evidence from the Cloud

In the United States, numerous constitutional and statutory provisions govern search and seizure, including that of forensic evidence from cloud providers. Since we focus on criminal cases, we will explore the Federal Rules of Criminal Procedure (FRCrP) and the Fourth Amendment. In this section we show how these statues might apply to acquisition of cloud-based ESI. We intend only to introduce the array of issues rather than to dive deeply into each one.

One statute plays an important part in cloud forensics: the Electronic Communications Privacy Act of 1986 (ECPA), codified at 18 U.S.C. §§2510-22. ECPA includes two definitions that are important when discussing cloud computing and the law. The first is an "electronic communication service" (ECS) that is "any service which provides to users thereof the ability to send or receive wire or electronic communications" (18 U.S.C. §2510). Title II of ECPA is referred to as the Stored Communications Act (SCA), 18 U.S.C. §2701-12, which adds the second definition. A "remote computing service" (RCS) that is "the provision to the public of computer storage or processing services by means of an electronic communications system" (18 U.S.C. §2711). Different rules apply to the two services, and a cloud provider might be an ECS or RCS or both, depending on the services it provides.

Search Warrants for Cloud Data

We now turn to the act of acquiring the evidence. In preparation for a full search warrant example, let us walk through some of the cloud-specific parts of the warrant.

The first part of a search warrant must describe what is to be seized. The law requires "reasonable particularity" in the description of the evidence, contraband, fruits, or instrumentality of crime that the agents hope to obtain by conducting the search.

In cloud computing environments, the "property to be seized" should contain a description of information (such as computer files) rather than physical hardware, regardless of the role of the computer in the offense. By definition, the physical hardware of a cloud provider is not owned by the suspect (unless the provider is the subject). Seizure of physical hardware yields no benefit that data alone cannot provide, and in fact may be disruptive to other cloud clients sharing that hardware. The "property to be seized" described in the warrant should fall into one or more of the categories listed in FRCrP Rule 41(b):

(1) "property that constitutes evidence of the commission of a criminal offense"

This is a very broad authorization, covering any item that an investigator reasonably believes would

[34] Couillard, D. A. (2009). Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing. *93 Minnesota Law Review*, 2205-2239.

reveal information that would aid in the investigation. "Property" has come to include tangible and intangible property. Case law has established that electronic data are also "property" that may be searched and seized.

(2) "contraband, the fruits of crime, or things otherwise criminally possessed"

In cloud environments, contraband could take one of the following forms. Contraband, including child pornography, pirated software, and other copyrighted materials, may be kept in cloud storage or inside of cloud virtual machines. When a hacker breaks into a machine hosted in the cloud, that machine could be the fruits of the crime – that property acquired as the result of the crime of unauthorized access.

(3) "property designed or intended for use or which is or had been used as a means of committing a criminal offense"

Cloud environments could be used as the instrument of a crime in several ways. Cloud storage could be used to transmit child pornography, and cloud-based virtual machines could be used to produce it. A virtual machine could be used for hacking, or used to host websites with illegal content. In each case, the cloud contains property used to commit an offense.

The second step in drafting a warrant is to describe the property's location. The law, rooted in the physical world, is interested in where the property is. The location, which must be noted with reasonable particularity, has historically been a safeguard to citizens that limit the scope of the warrant. Search warrants for online webmail have traditionally specified only the email address as the "place to be searched." "Location" requires special consideration when dealing with online data, especially with cloud computing. Only rarely will data be stored on a single server at the address of the data custodian. In many cases the servers will be dispersed across state or international boundaries. Further, cloud data are often replicated to multiple datacenters. This seemingly presents a problem when describing the "location to be searched," since the agent or prosecutor may not know where the data containers are.

The search warrant for cloud-based data should not specify a physical address to be searched, lest the search exclude data stored at other physical locations. Instead, the warrant should specify the desired data and the warrant served to the data custodian.

Here is an example of how to describe the location of cloud-based data in some datacenter owned and controlled by Amazon:

> *Data, metadata, and account information created, stored, or controlled by Amazon Web Services LLC, 410 Terry Avenue North, Seattle, WA 98109-5210, related to IP address 1.2.3.4 for the time period beginning 12:01 a.m. CST (January 1, 2012) through 12:01 a.m. CST (July 1, 2012).*

> *The terms "data" and "metadata" include all of the foregoing items of evidence in whatever form (such as virtual machines, user-created content, log data, packet captures, intrusion detection alerts, billing records) and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as volatile and non-volatile information on an electronic or magnetic storage device, including hard disks, backup storage, live memory, as well as printouts and readouts from any storage device), in any physical location controlled by the provider where the data may reside.*

The third step in drafting a warrant is to set the parameters for executing the warrant. Federal warrants allow the specification for the time of day during which to execute the warrant, and the date by which to execute the warrant. These are further safeguards to ensure a limited lifetime of the warrant and minimal disruption (*e.g.* "in the daytime between 6:00 a.m. to 10 p.m.") to the subject of the warrant.

The elasticity and near-instant provisioning and de-provision of data poses a legal challenge in cloud computing. Unless physical machines are seized or virtual machines are turned off, execution of the warrant is unlikely to impact or disrupt the data owner, but in fact risks spoliation if announced. The search warrant can be executed at any time in the day or night, but should be executed as soon as possible to preserve evidence. The traditional response time of 10 days should be shortened as much as possible, within reason of the logistical constraints of the cloud provider.

An affidavit to justify the search and seizure of cloud-based computer data should include, at a minimum, the following sections: (1) definitions of any technical terms used in the affidavit or warrant; (2) a summary of the offense, and, if known, the role that a targeted computer plays in the offense; and (3) an explanation of the agents' search strategy.

While agents and prosecutors should resist the urge to pad affidavits with long, boilerplate descriptions of well-known technical phrases, cloud computing is a new discipline and currently requires special attention to defining new terms. As a rule, affidavits should only include the definitions of terms that are likely to be unknown by a generalist judge and are used in the remainder of the affidavit. Figure 2 shows a sample definition for "cloud computing" which could be used in the affidavit. This, and several others, are included in the sample search warrant later in the chapter.

Virtual Machine ("VM")

Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a virtual machine ("VM"), does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.

Figure 1. Definition of "Virtual Machine" for use in a search warrant.

These concepts are embodied in the sample search warrant that follows. The key thing to remember is that the seizure should focus on data rather than hardware, and that the data may be distributed across physical locations.

Case Study

To illustrate the application of the concepts presented so far, we will now look at a hypothetical case study of a cloud-based crime. This case study was previously used to explain technical issues in cloud forensics.[35] After analyzing the scenario, we can then construct a sample search warrant that could be used in this case.

Here is the hypothetical crime:

> *Polly is a criminal who traffics in child pornography. He has set up a service in the cloud to store a large collection of contraband images and video. The website allows users to upload and download this content anonymously. He pays for his cloud services with a pre-paid credit card purchased with cash. Polly encrypts his data in cloud storage, and he reverts his virtual webserver to a clean state daily. Law enforcement is tipped off to the website and wishes both to terminate the service and prosecute the criminal.*

This is a case where the computer is incidental to the offense. Let us assume that this scenario took place in Amazon EC2. Let us assume that law enforcement first contacts the cloud provider with a preservation order to retain evidence pending a warrant. Preservation is authorized under 18 U.S.C. §2703(f)(1) which says "A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." Tracking down the user is the more difficult task.

The examiner has no technical ability to image the virtual machine remotely since the cloud provider does not expose that functionality, and in doing so would alter the state of the machine. Deploying a

[35] Dykstra, J. & Sherman, A.T. (2011). Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies. *Proceedings of the 2011 ADSFL Conference on Digital Forensics, Security, and Law*, 191-206.

remote forensic agent, such as EnCase Enterprise, would require the suspect's credentials, and functionality of this remote technique within the cloud is unknown. Simply viewing the target website is enough to confirm that the content is illegal, but it tells us nothing about who put it there. Additionally, no guarantee can yet be made that the target webserver has not been compromised by an attacker, or that the examiner's request to the web server was not the victim of DNS poisoning, man-in-the-middle, or some other alteration in transit.

Consider other possible sources of digital evidence in this case: credit card payment information, cloud subscriber information, cloud provider access logs, cloud provider NetFlow logs, the web server virtual machine, and cloud storage data. Assistance from the cloud provider is paramount here. Law enforcement can issue a search warrant to the cloud provider, which is adequate to compel the provider to provide any of this information that they possess. Law enforcement need not execute or witness the search. The warrant specifies that the data returned be an “exact duplicate,” the forensic term that has historically meant a bit-for-bit duplication of a drive. Since child pornography is a federal offense, the provider must comply with the order. A technician at the provider executes the search order from his or her workstation, copying data from the provider's infrastructure and verifying data integrity with hashes of the files. Files may have been distributed across many physical machines, but they are reassembled automatically as the technician accesses them. Though the prosecution may call the technician to testify, we have no implicit guarantees of trust in the technician to collect the complete data, in the cloud infrastructure to produce the true data, nor in the technician's computer or tools used to collect the information correctly. Nonetheless, the provider completes the request, and delivers the data to law enforcement.

To reconstruct the crime, the forensic investigators need evidence to help them piece together the following:

- A copy of the virtual machine in order to understand how the web service works, especially how it encrypts/decrypts data from storage;
- Keys to decrypt storage data, and use them to decrypt the data;
- Copies of all files in order to confirm the presence of child pornography; and
- Cloud access logs or NetFlow to identify possible IP addresses of the criminal.

By viewing the website it is clear that it contains illegal content, but not who the data owner is. Timestamps and other file metadata may prove useful, provided they are available and accurate. For this reason, complete bit-for-bit copies of the original evidence are important.

Case Study Search Warrant

The following pages present one example of an application for a search warrant in the hypothetical case study. Note how the request focuses on data rather than on hardware. For this reason, it is written as an ECPA §2703(d) warrant. An FRCrP Rule 41 warrant would have been used to seize

hardware or imaging disk drives on-site. A template warrant can be found at http://cisa.umbc.edu/warrant/. The document is an academic example that illustrates the issues above.

Paragraph 1 establishes the request for cloud data in investigation of the crime. Paragraph 4 details the cloud crime and presents probable cause that the provider has relevant evidence. The technical background in paragraphs 5-12 is specific to cloud computing, using Amazon as the example. They describe how the service works and what data may be available. Paragraphs 13-23 are similar to language found in any request for electronic evidence.

Conclusion

Cloud computing is an advancement in the history of computation due in large part to the convergence of technologies. The economics of the paradigm will drive growth and adoption rates from companies and individuals. Where the people, the data, and the money go, so does crime. While investigators struggle with the new problems of acquiring and analyzing cloud data, the law must prepare for the legal challenges associated with acquiring and presenting cloud data in court. The first public cases involving cloud-based ESI are likely to appear soon, and the people involved in those cases have a unique opportunity to set a new legal precedent.

When these cases emerge, each player's actions will be shaped by an interpretation of how traditional discovery rules govern the cloud crime. As we saw, applying these rules can be murky and unclear. Preservation, ownership, jurisdiction, and search warrant execution are just some areas where we saw non-trivial challenges.

Examining a concrete case study helped highlight the practical implication of the complex considerations for acquiring evidence. However, the case study introduced a context against which to build a search warrant. As a first public example, this language arms law enforcement agents with topics to consider when they draft their first warrant for cloud data.

Now is an exciting time for cloud computing as innovative new product offerings emerge. The legal community is also at the threshold of a wave of cloud-based crimes. Our exploration of seizing electronic evidence from cloud computing provides a foundation to forensic investigators and legal professionals as they investigate and prosecute of cloud-based crimes.

*Dr. **Josiah Dykstra** is a recent graduate of the University of Maryland, Baltimore County where his PhD research focused on the technical and legal challenges of digital forensics for cloud computing. His other research interests include network security, intrusion detection, and malware analysis. Dr. Dykstra received a B.S. in computer science and a B.A. in music from Hope College. As part of the NSF Scholarship for Service, he earned an M.S. in information assurance from Iowa State University. Dykstra is employed by the US Department of Defense. He is a member of the ACM, IEEE, American Academy of Forensic Sciences, Cloud Security Alliance, NIST Cloud Forensic Science Working Group, IFIP Working Group 11.9 on Digital Forensics, and American Bar Association E-Discovery and Digital Evidence Committee.*

2013 (2H) Information Law Updates: Cases, Statutes, and Standards

By Thomas Shaw

In the second half of 2013 and the end of the first half, there have been many developments in U.S. and international information security and privacy statutes, cases and standards. This includes international and U.S. state and federal laws and regulations that have been passed or are coming into force. It also involves civil and criminal cases and enforcements actions brought by regulators. And it encompasses the new standards, guidelines and legal ethics opinions in this area. But it leaves out cases on recurring themes and it does not attempt to track legislation that has not been passed. To briefly summarize the major developments in this area of law and practice, each significant development is presented with a brief analysis after it. Deeper analyses of these developments can be found in other articles in this publication and in writings and presentations by members of the Information Security committee.

These developments are categorized as:

- Statutes and Regulations – U.S.
- Statutes and Regulations – International
- Cases – Civil and Criminal
- Cases – Regulatory
- Standards and Guidelines

Statutes and Regulations – U.S.

Employer Requests for Social Networking Data[1]

Joining almost a dozen other states, Utah, Washington, Nevada, and New Jersey have passed laws that both restricts the ability of employer to request personal social network login credentials from prospective or current employees, while at the same time providing the employers the ability to request from employees such information under certain situations. For Utah, this includes for any devices or accounts provided by the employer. Employees can be terminated when an employee's personal account is being used to steal the employer's proprietary information. Employers can block employee access to such sites on employer provided devices. Washington's law allows requests for profile content, not login credentials, under certain circumstances, including employer investigations but does not allow employers to force employees to "friend" them or allow adverse actions against

[1] Utah, Internet Employment Privacy Act (Apr. 2013); Washington, An Act Relating to social networking accounts and profiles (May 2013); Nevada, An act relating to employment; prohibiting employers from conditioning employment on a consumer credit report or other credit information; providing certain exceptions; prohibiting employers from conditioning employment on access to an employee's social media account; providing civil remedies and administrative penalties; and providing other matters properly relating thereto (June 2013); New Jersey, An Act prohibiting the requirement to disclose personal information for certain electronic communications devices by employers (Aug. 2013).

employees for refusal to provide login credentials to personal social networking sites. Nevada's law narrowly focuses on asking for personal social media login credentials and retribution for refusal of such.

California Privacy Law Revisions[2]

The legislature in California passed five different bills related to privacy in the current session. The first is an amendment to the state's Online Privacy Protection Act by requiring websites or mobile apps to disclose in their privacy policies how they respond to browsers that have the Do Not Track feature enabled and if third parties can collect consumer PII on the sites/apps. The second is requires that websites including social media and mobile apps allow the content about minors to be removed and advertising to minors be limited to products that they can legally purchase. The third would require a warrant for an electronic communications (e.g. emails, tweets, Facebook messages and posts) regardless of whether it has been read or not or its age (in contrast to the arcane rules under the federal SCA). The fourth expands the definition of personal information for data breach notification to include unencrypted credentials for an online account, including the userid (possibly an email address) and password, security question and answer. The fifth expands the protection of ePHI to all those organizations maintaining ePHi and includes mobile apps in this protection requirement.

Statutes and Regulations – International

China Privacy Rules[3]

The Chinese government, through the Ministry of Industry and Information Technology, has issued finalized rules targeting ISPs and their consumers. These rules help to define what is considered personal information and the requirement that ISPs and websites are to discontinue the use of such information when the consumer is no longer using their services. ISPs and website are required to get consent before legally collecting personal information, to not use such information for purposes beyond which it was collected, and to not collect information that is does not need to provide the services. They are to inform consumers of the processing done on the information and to safeguard the information. They are not to disclose or sell consumer information to third parties and are responsible for oversighting third-party subcontractors. Violators are to be reported to the government for action and subject to fines. This is in addition to other recent rules, decisions and statutory revisions strengthening online consumer protection rights in China through regulation of online marketplaces, infosec guides for government and non-governmental systems, opinions on the consuming of information, and revisions to longstanding consumer protection laws.

[2] California, AB 370, SB 568, SB 467, SB 46, AB 658 (Sept. 2013).
[3] China, Rules on the Protection of Personal Information of Internet and Telecommunication Users (July 2013).

Cases – Civil and Criminal

U.S. v. Nosal[4]

Another link in the long chain of this case, especially as it relates to the CFAA, came with the conviction of David Nosal on charges of using illicit means to acquire the information of a former employer. Previously, the Ninth Circuit first provided a wider interpretation of the CFAA, that it included the actions where an insider exceeded their authorizations to this corporate information. On rehearing en banc, the Ninth Circuit provided a more narrow interpretation, that the CFAA was intended to deal with third-party hackers and did not include insiders exceeding their authorizations to steal trade secrets and other confidential information (i.e. it was aimed at outside hackers, not inside misappropriators). In this trial, Nosal was convicted of having former employees use deceitful means to get access details from insiders to provide him with corporate information. So while he was not an insider, he was not a hacker, but this conduct into a third category of an outsider who used deceit to acquire corporate information illicitly from insiders.

U.S. v. Connor[5]

The Sixth Circuit rejected a contention from a convicted receiver and possessor (taken of his own child) of child pornography that police use of peer-to-peer software was a Fourth Amendment violation. The court stated that the expectation of privacy had to be both actual and reasonable but the expectation failed because not "one society is prepared to recognize as reasonable." The court differentiated its ruling from *Warshak*, because file sharing is different than email. This is because peer to peer software is intended to make is files available to others, while ISPs are merely incidental recipients of the emails passing through their systems. The user of peer to peer software voluntarily exposed his files to public access and therefore could have no reasonable objective expectation of privacy in them. Even the subjective intention to not share files by hiding them does "not create an objectively reasonable expectation of privacy in the face of [the] widespread public access" The court ruled that police were intended recipients, as were all others using this peer-to-peer software, of any files that had been marked for sharing. Unlike the ISPs incidental access to information, the police as users of this software were not incidental accessors, but intended, and as such upheld the conviction.

comScore Class Certification[6]

Using allegations that the gathering of data from end-user computers that exceeded the consent given and the CFAA, ECPA, and the SCA federal statutes, a district court has granted class certification against comScore. The company's OSSProxy software is downloaded typically in a bundle with other free software and monitors and collects and forwards a vast amount of information, including not only Internet activity, but the names of all files on the subject computer and contents of PDFs found there. In the common question prong of class certification, the court looked to the interpretation of the User

[4] *U.S. v. Nosal*, Case No. CR 08-0237 (N.D. Cal. Apr. 2013).
[5] *U.S. v. Connor*, Case No. 12-3210 (6th Cir. Apr. 2013).
[6] *Harris and Dunstan v. comScore, Inc.*, Case No. 11C5807 (N.D. Ill. Apr. 2013).

License Agreement (a form contract) to provide the requirement for a common question, focusing for example on the consent provided therein. Rejecting defendant claims that such consent was subjective and therefore different to each user, the court held that the approval and downloading experiences and ULA were common and therefore objective based on this common conduct.

Siegler v. Best Buy[7]

The Eleventh Circuit has affirmed a lower court's ruling on the applicability of the Driver's Privacy Protection Act (DPPA). A Best Buy customer returned an item to the store and the magnetic strip of his driver's license was scanned into a Best Buy system with his approval (the strip contains the same data as the front of the license). He asked that the information be deleted but was refused and so brought suit under the DPPA. The court agreed that the law was intended to prevent disclosure of driver's license data from a government agency, not from the driver's license holder himself. The invoice for the original purchase had stated on it that proper identification would be required upon the return of items, meaning that the customer was properly notified of the use of his driver's license.

Sams v. Yahoo! [8]

The Ninth Circuit rejected an appeal by a plaintiff who alleged violations of the SCA. This was based on Yahoo! producing data on the plaintiff based on responding in good faith to a grand jury subpoena. The court said that the good faith defense under SCA would be available if the subpoena was valid on its face and the defendant had no knowledge of it being invalid or irregular. Yahoo! had produced basic subscriber (non-content) information about the plaintiff, allegedly in violation of state law. The court did not address the violation of state law question, finding that Yahoo!'s good faith production qualified it for the defense under the SCA. It did reject the contention that by producing the information before the deadline, Yahoo! had committed an unlawful voluntary disclosure.

<u>Geolocation Data Cases</u>

New Jersey v. Earls[9]

The supreme court of the state of New Jersey has ruled that there is a right to privacy for cell phone geolocation data under the New Jersey constitution. To locate a criminal suspect potentially threatening a cooperating witness, police had used cell-tower location data to trace the suspect's location and arrest him. They had done so without obtaining a warrant. Based on a concern for the threat to individual privacy rights, such as possibly mapping of the daily routine and places visited of a cell phone owner, the court held that the New Jersey constitution does not allow such warrantless searches. Reviewing federal cases, it showed that the state's constitution provides more protection against unreasonable searches and seizures than the Fourth Amendment of the U.S. Constitution,

[7] *Siegler v. Best Buy Co. of Minn., Inc.*, Case No. 12-13719 (11th Cir. Apr. 2013).
[8] *Sams v. Yahoo! Inc.*, Case No. 11-16938 (9th Cir. Apr. 2013).
[9] *New Jersey v. Thomas W. Earls*, Case No. 068765 (N.J. July 2013).

which has been variously interpreted. But because this decision only applies to state and not federal law, the scope of this is confined to this state.

U.S. Government Request[10]

The Fifth Circuit Court of Appeals overturned a lower court ruling that the government requesting geolocation data on cell phones from telecom providers under the SCA in regard to criminal prosecutions was unconstitutional. The lower court had held this Fourth Amendment violation occurred because the SCA allows for the "specific and articulable facts, rather than probable cause." The court of appeals focused on the fact that the government was not the one collecting the location information, the telecom companies were. The court differentiated content information between two content subscribers from this non-content information that was from communications between a subscriber and the service provider, which it found subject to the business records exception. It also agreed that this information is provided voluntarily by the subscriber to the telecom company. As such, there could be no reasonable expectation of privacy in these business records and no constitutional violation.

_____

Genesco v. Visa[11]

In this case, a retailer is seeking rebate of $13m in fines and penalties imposed by VISA on the retailer's bank for costs associated with the data breach of Genesco's system. Hackers intercepted unencrypted communications of during cardholder purchases as they were being transmitted to the banks. Visa had assessed over $5m in operating expense recovery and fraud recovery under an ADCR (Account Data Compromise Recovery) process for the U.S. and $8m under a DCRS (Data Compromise Recovery Solution) process internationally. Genesco claims that the accounts that were altered were not impacted by the data breach based on its forensic evidence and so Visa's costs reclamation far exceed the actually damage of the breach. If furthers alleges that the PCI DSS standard that merchants are required to adhere to allows for unencrypted data to be sent during the transaction approval process, so Genesco was in compliance with PCI DSS during the time of the breach.

Lazette v. Kulmatycki[12]

The plaintiff here alleges that the defendant, her supervisor at a previous job, after taking back her cell phone upon her departure from the company, proceeded over an eighteen month period to read tens of thousands of emails on her personal account through her corporate cell phone. In the motion to dismiss, the court overruled a number of objections, including that the SCA did not apply in this case because it had been intended to apply only to hackers, that the supervisor had access because he accessed the emails from a company owned device, that the plaintiff gave consent to access the emails by not deleting her account, and that emails read by the defendant before the plaintiff were no longer

[10] *In re: Application of the U.S. for Historical Cell Site Data*, Case No. 11-20884 (5th Cir. July 2013).
[11] *Genesco, Inc. v. Visa, USA, Inc.*, Case No. 3:13cv202 (M.D. Tenn. July 2013).
[12] *Lazette v. Kulmatycki*, Case No. 3:12CV2416 (N.D. Ohio June 2013).

in electronic storage and so protected. But those emails that were opened first by the plaintiff and then read by the defendant were not subject to protection under the SCA.

Ehling v. Monmouth-Ocean[13]

In this case, the images from the Facebook wall of the plaintiff criticizing the defendant organization were turned into the company by a co-worker and Facebook friend of the plaintiff. Among other contentions were that these private posts on the Facebook wall were not public and so were protected under the SCA. The court agreed that the postings were electronic communications, transmitted by an ECS, in electronic storage and intended to be private and so were protected under the SCA. Because the posting were provided to the company by the co-worker who was authorized to view the posts, under no coercion from the company, the company was not held to be liable under the SCA. The NLRB, after the plaintiff had previously filed a complaint there, had also ruled that the actions of the corporation had not violated the National Labor Relations Act.

Google Privacy Cases

Email Scanning[14]

In the first case under the Wiretap Act, Google is being sued regarding its interception and scanning of emails in its Gmail system, to be able to provide applicable advertisements to the recipient of the email and also to create profiles of users for other Google services. The plaintiffs contend that the interception of the emails violated the Wiretap Act. Google denied that based on the ordinary course of business exception and consent given by the users of the Gmail service. The court disagreed, as the exception is available when the interception is were "an instrumental part of the transmission of email." Google contended that by agreeing to its terms of service, the Gmail user explicitly consented to interception but the court did not find that the terms of service and privacy polices explicitly notified users of that Google would be doing with their emails. Google also said that the non-Gmail users implicitly consented by sending an email to Gmail users. The court did not accept this argument either and denied Google's motions to dismiss based on either theory.

Street View Wi-Fi Scanning[15]

In a second case under the Wiretap Act, related to unencrypted data collected by Google during its collection of Street View data, the court of appeals affirmed the decision of the lower court that Wi-Fi transmissions are not electronic communications that are readily accessible the public. More specifically, unencrypted payload data sent over a Wi-Fi network are not radio transmissions as defined under the Act and are not generally accessible to the public, due to their limited range and the need for sophisticated hardware and software to intercept these transmissions.

---

[13] *Ehling v. Monmouth-Ocean Hospital Service Corp.*, Case No. 2: 11-cv-03305 (D. N.J. Aug. 2013).
[14] *In re Google Inc. Gmail Litigation,* Case No. 13-MD-02430 (N.D. Cal. Sept. 2013).
[15] *Joffe v. Google Inc*., Case No. 11-17483 (9th Cir. Sept. 2013).

Cookie Placement[16]

In the third suit, plaintiffs were seeking to show that the collection of their personal information through the unconsented placement of cookies by Google and advertisers showed that they suffered economic loss. Despite showing that was economic value to the PII related to web browsing activity, the court ruled that they had not demonstrated that its value had been impaired by being made available to third party marketers to perform targeted advertising and therefore did not have the requisite Article III standing. But because statutory violations could provide that standing, the court analyzed the allegations under federal and state laws. For example, under the Wiretap Act, it did not view URLs as contents, such that even if Google did not obtain these URLs with user consent, receiving the URLs was not considered a prohibited interception of an electronic communication. And the lack of economic loss described above precluded CFAA claims.

Safari Third-party Cookies[17]

In the fourth suit, thirty-seven states had pursued claims that Google had overridden the privacy settings of the Safari browser that allow for blocking third-party cookies. To settle these allegations, Google agreed to pay $17m and not use the HTTP POST function to override cookies blocking settings to place a cookie on users' computers. Google also agreed to tell users how to expire any of these cookies that were set and maintain a "cookies" webpage that explains its use of cookies.

Chaney v. Fayette School District[18]

A bikini-clad photo of a teenage from her Facebook page was the focus of a suit against the school district and its employees and leaders who sanctioned its use in a presentation on the dangers of the Internet. Used in a presentation to the public about how images once on the Internet can be there long after they may not be desired to be by the poster of the image, and presented next to an image of a mother who regretted her earlier decisions, the plaintiff alleged violations of her Fourth Amendment rights to privacy. The court said that the then teenager, while she may have a subjective expectation of privacy, could have no objective privacy right recognized by society, because of her privacy settings, which were the broadest available for those her age. She had allowed her Facebook page where the photo was posted to be viewed by friends and friends' friends and because she could not control who the friends' friends were, she had giving viewing to third parties and given up her objective expectation of privacy.

U.S. v. Katzin[19]

The use of location data gathered from a GPS tracker attached to the vehicle of a criminal suspect but installed without a warrant was an unlawful search under the Fourth Amendment. The government

---

[16] *In re: Google Inc. Cookie Placement Consumer Privacy Litigation*, Case No. 12-2358 (D. Del. Oct. 2013).
[17] *In the matter of Google Inc.*, Assurance of Voluntary Compliance (Nov. 2013).
[18] *Chaney v. Fayette County Public School District and Cearley*, Case No. 3:13-cv-89 (N.D. Ga. Sept. 2013).
[19] *U.S. v. Katzin*, Case No. 12-2548 (3rd Cir. Oct. 2013).

contented that a warrant was not needed and in any case the good faith exception to the exclusionary rule should apply, as its actions occurred before the ruling in *U.S. v. Jones* declaring the attachment of a GPS device to be a search. The court of appeals differentiated the capabilities of beepers who evidence had previously been allowed by courts to the more intrusive and not time or geography limited nature of GPS trackers. Using a GPS tracker of such information gathering capabilities required a warrant before attaching. The government identified three types of cases where a warrant was not required but the court ruled that reasonable suspicion, except if very specific circumstances, could not justify the attachment of the GPS tracker without a warrant. A warrantless search based on probable cause under the automobile exception was not applicable here. Good-faith reliance on the rulings from other circuits holding that a warrant was not required for GPS trackers were not sufficient to allow for an exception to the exclusionary rule. The court ruled that the evidence was properly suppressed.

Curry v. AvMed[20]

Health insurer AvMed settled a class-action lawsuit against it relating to a data breach of the unencrypted information of more than one million customers. The plaintiffs had previously prevailed in a motion to dismiss, because of possible links between the data breach and instances of identity theft. The led to the $3m settlement, based on the theory that the defendants were unjustly enriched because the members of the class had paid part of the insurance premiums based on receiving adequate data security protections, which the breach exposed as inadequate. Those who suffered identity theft from the breach were part of a separate settlement class. The company was also required to implement a rigorous information security program.

Alberta v. United Food and Commercial Workers[21]

The Supreme Court of Canada has ruled that the privacy law of the province of Alberta is unenforceable and must be changed within twelve months or become invalid (in which case the national privacy law would then take precedence). The province's Personal Information Protection Act was found to be in violation of the Canadian Charter of Rights and Freedoms. The case involved workers who crossed a picket line during a labor dispute being photographed and videotaped by both the union and the employer involved and their images potentially posted online. Upon complaints from those so recorded, the province's privacy commissioner ruled that the photography was against the privacy statute but the trial, appeal, and Supreme Court all found that the public nature of the legal and protected labor action for collective bargaining was such that no right of privacy could be invoked and the statute did not have sufficient exceptions for these types of situations. The Court found that the law overbroad in that it "limits the collection, use and disclosure of personal information other than with consent without regard for the nature of the personal information, the purpose for which it is collected, used or disclosed, and the situational context for that information." Specifically that the privacy law was not constitutional to the extent that it "restricts collection for legitimate labour

[20] *Curry and Moore v. AvMed, Inc.*, Case No. 10-cv-24513 (S.D. Fla. Oct. 2013).
[21] *Information and Privacy Commissioner of Alberta v. United Food and Commercial Workers, Local 401*, Case No. 34890 (Canada Nov. 2013).

relations purposes." Alberta's privacy law is similar to others in Canada, so possibly mandating revisions to multiple Canadian provincial privacy laws.

Cases – Regulatory

HHS and Idaho State University[22]

HHS settled its case against Idaho State University for its oversight of the information security related to 29 family medicine clinics. In finding that the university had exposed ePHI, it showed that the university had failed to properly implement the HIPAA Security Rule and effective security measures. This included leaving ePHI exposed for almost a year through disabled server firewalls, not performing appropriate risk assessments, and not performing regular reviews of risks or vulnerabilities that may have caught this problem. The agreement included a corrective action plan to last for two years.

HHS and Shasta RMC[23]

HHS settled its investigation into Shasta Regional Medical Center for violations of the HIPAA Privacy Rule. This was for disclosure of a patient's PHI by senior leaders of the organization to news media outlets and within the organization without the consent of the affected patient, as well as not disciplining any staff members for the disclosures. This was in response to contentions raised about a possible case of Medicare fraud, which the medical center was trying to disprove. In addition to a significant fine, a corrective action plan was agreed that also extends to more than a dozen other medical centers or hospitals that are under the same ownership or operational control.

Google and Spanish DPA[24]

The advocate general of the European Court of Justice issued a non-binding opinion in this case involving Google and the Spanish data protection authority. The original case involved the electronic format of 15-year-old newspaper articles about the plaintiff that he no longer believes should be the result of search results. These involved attachment of his property for debts that has since been resolved. The opinion looked at three questions involving the application of the European DPD to search engines. The most significant of those questions was whether the DPD would apply to search engines that did not process data inside the EU. The opinion was that the focus for analyzing jurisdiction for search engines should not be on the location of the processing but the location of the offices of advertisers who were selling keywords used on the search engine targeting the consumers of a specific country. The opinion also concluded that DPAs could not in most cases compel the removal of data from search engine indices, as they were not controllers of the data. And that there is no general right to be forgotten under the DPD so it cannot be invoked against search engines.

---

[22] *HHS and ISU*, Resolution Agreement (May 2013).
[23] *HHS and Shasta Regional Medical Center*, Resolution Agreement (June 2013).
[24] *Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD)*, Opinion of Advocate General, European Court of Justice (June 2013).

HHS and WellPoint[25]

HHS settled with WellPoint, including a fine of $1.7m, for exposing the ePHI of over half a million patients on the Internet. These violations of the HIPAA Security Rule included lacking necessary technical and administrative controls regarding the database containing this ePHI. The specifics involved the process to provide authorization to the database, the controls regulating verification of the access to the exposed database, and for technical evaluations related to upgrades in software used in this system.

HHS and Affinity Health[26]

HHS settled its investigation into Affinity Health for violations of the HIPAA Privacy and Security Rules, including a fine of more than $1m. This involved the disclosure of ePHI of more than 300,000 people, whose information was still on the digital copiers which were returned to the lessors. Covered entities are required to take into account such risks when assessing risks and vulnerabilities. It also did not delete the ePHI before returning the copiers, which was discovered as part of a news program on the risks of digital copy machines. Affinity entered into a corrective action plan as part of the resolution agreement.

U.S. v. TRENDnet[27]

The FTC settled its action against TRENDnet over its information security practices. The defendant sells cameras that allow remote viewing over the Internet. Despite claims of secure access and logins, the company was alleged to have sent its authentication information over the Internet in the clear, stored authentication information for its mobile device app in the clear, failed to review its provided software for security vulnerabilities, or take into account third-party security vulnerability reports. This led to hackers being able to view all the live feeds that were supposedly secured on the company's websites, including many of children in their homes.

U.S. v. Aaron's[28]

The FTC settled its action against Aaron's Inc. over allegations that they national rent to own store assisted franchisees with installing the capability to use webcams and screen shots to monitor the activities of equipment renters. In addition, keyloggers that captured sensitive financial and other access credentials were captured. Beyond being able to disable computers remotely, Wi-Fi information of the location of the computer was also captured. These unfair act or practices in violation of the FTC Act, which were the subject of previous actions against the designer of the software used, were settled by Aaron's agreeing not to capture keystrokes or screen shots or activate the camera or microphone of a rented computer and to give notice to the use of location tracking technologies.

---

[25] *HHS and Shasta Regional Medical Center*, Resolution Agreement (June 2013).
[26] *HHS and Affinity Health Plan, Inc.*, Resolution Agreement (Aug. 2013).
[27] *In the matter of TRENDnet, Inc.*, FTC File No. 112 3090 (D.D.C. Sept. 2013).
[28] *In the matter of Aaron's Inc.*, FTC File No. 132 3156 (Oct. 2013).

Standards and Guidelines

SEC/CFTC Identity Theft Rules[29]

The SEC and the Commodity Futures Trading Commission (CFTC) issued final rules for identify theft programs for those entities that they are regulate, under Dodd-Frank. The respective financial institutions and creditors are required to develop and implement identity theft programs that "detect, prevent, and mitigate" these risks for their covered accounts. Specifically, the programs need to identify and detect relevant red flags, prevent and mitigate identity theft, and review and update the program.

NIST Security Controls[30]

NIST has released the final version of the latest release to its information security and privacy controls document for federal systems. Controls and control enhancements were added in this release to address: mobile and cloud computing; applications security; trustworthiness, assurance, and resiliency of information systems; insider threat; supply chain security; and the advanced persistent threat (APT). As previously discussed, privacy controls were added in a new appendix to align with the Fair Information Practice Principles. There are also additional tools to assist organizations in customizing control baselines to their specific situation.

NIST Mobile Device Security[31]

NIST published its guide to deal with the centralized security management of smart mobile devices. It identified the threats and vulnerabilities of these devices as untrusted devices, networks, applications, and content, missing physical security controls, interactions with other systems, and use of location services. To address these threats and vulnerabilities, it recommends having mobile device security policy, develop threat models for these devices, implement necessary security services, use of encryption in transmissions and storage, use of device authentication, restricting apps, performing testing of changes before production, perform regular security maintenance, and secure every remote device before allowing use.

DAA Mobile Guidelines[32]

The Digital Advertising Alliance (DAA) has published guidance for applying the previously promulgated self-regulatory principles for online behavioral advertising and multisite data to mobile devices websites and apps. The principles areas addressed are for the transparency and control over multisite data, cross-app data, precise location data, and personal directory data. There is additional coverage for limitations for operations and systems management, marketing research or product development

---

[29] SEC, 17 CFR 248 subpart C, *Regulation S-ID: Identity Theft Red Flags* and CFTC, 17 CFR 162 subpart C*, Identity Theft Red Flags* (Apr. 2013).
[30] NIST, SP 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).
[31] NIST, SP 800-124r1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (June 2013).
[32] DAA, *Application of Self-Regulatory Principles to the Mobile Environment* (July 2013).

and restrictions on data collection and use for employment, credit, insurance, and health care eligibility and health and financial data.

NTIA Mobile App Code of Conduct[33]

The Department of Commerce's National Telecommunications and Information Administration has published its mobile app short form notice. This is intended to provide consumers with more information about their data that is collected and possibly shared with third parties by mobile apps. In addition to transparency about the data collected and shared, the design of the short form is described considering the different device types the short form will be displayed upon and links to long form policies.

OECD Privacy Principles[34]

The OECD has revised its 1980 guidelines on privacy and transborder data flows. Revisions include a new of new sections. Part III addresses the implementation of accountability, in how the data controller should undertake a privacy management program. Breach notification is called for using a risk-based approach. Privacy enforcement authorities and laws protecting privacy are strongly recommended as necessary, as part of national implementation, along with a national privacy strategy and coordination across governmental agencies. Transborder data flow guidelines have been modernized. Awareness training, privacy credentials, and privacy enhancing technologies are all recommended to assist with strengthening privacy protections. Increased global cooperation and interoperability are called for.

NIST Cybersecurity Framework[35]

NIST release a draft version of the framework for cybersecurity for critical infrastructure. This follows on from an executive order issue by the president earlier this year calling for such a framework. The framework document gives organizations the a mechanism along with common language to: "1) describe current cybersecurity posture; 2) describe their target state for cybersecurity; 3) identify and prioritize opportunities for improvement within the context of risk management; 4) assess progress toward the target state; 5) foster communications among internal and external stakeholders." It has three parts that cover core best practices and standards, implementation tiers (Partial, Risk-Informed, Repeatable, Adaptive), and profiles specific to each organization's use of the functions (Identify, Protect, Detect, Respond, Recover) and the categories (e.g. data security, access control) and sub-categories within each function.

[33] NTIA, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices* (July 2013).
[34] OECD, *Guidelines governing the protection of privacy and transborder flows of personal data* (July 2013).
[35] NIST, *Preliminary Cybersecurity Framework* (Aug. 2013).

HIPAA Notices of Privacy Practices[36]

HHS and its offices (OCR and ONC) have released model notices of privacy practices for health care providers and health plans to consider using when creating their HIPAA required notices. HIPAA requires these covered entities to provide notice of both their privacy practices and the privacy rights of consumers, in simple languages. The notices are for both types of covered entities and come in four different formats.

FDA Mobile Medical Apps Guidance[37]

The FDA has released final rules on mobile medical apps, which are defined as a device under and the Federal Food, Drug, and Cosmetic Act and either assists a regulated medical device or allows a mobile device to become a regulated medical device. Not all mobile apps in the medical field will be regulated, including those that a related to general functions (e.g. advice, research, or medical office support) or have a lower safety impact (e.g. motivating the performance of physical therapy). Those apps that will be regulated then are those that qualify as a device and could pose a risk to patient safety if it does not work as intended.

Article 29 WP Cookie Consent[38]

The Article 29 Data Protection Working Party has put out a working document in regards to obtaining the necessary consent for Internet cookies. Following on from the requirements of the e-Privacy Directive and its own opinion on consent, the Working Party examined the following four areas: specific information, timing, active choice, and freely given. This includes that the information must be presented "before the cookies are set or read." A positive action of choice should be taken close on the screen to where the information is presented. It is recommended that users be given a meaningful choice accept only some of the cookies, if so desired, and not make general access predicated on accepting all cookies. Real choice must be offered in regards to tracking cookies.

PCI DSS New Version[39]

The Payment Card Industry's Security Standards Council has released v3.0 of the Data Security Standard. This provides a series of clarifications, evolving requirements, and additional guidance on the standard. Some of the new requirements include the need to include diagrams depicted cardholder data flows, an inventory of in-scope system components, that antivirus programs are running and cannot be disabled, protections against broken authentication and session management, unique authentication credentials for each customer, physical access controls, tampering and substitution controls for devices capturing payment card data, all root/superuser access must be logged, as are any ability to stop or pause audit logging, incident response technique for unauthorized wireless access points, penetration testing methodology, that risk assessment should be performed

---

[36] HHS, *Model Notices of Privacy Practices* (Sept. 2013).
[37] FDA, *Mobile Medical Applications - Guidance for Industry and Food and Drug Administration Staff* (Sept. 2013).
[38] Article 29 DPWP, *Working Document 02/2013 providing guidance on obtaining consent for cookies* (Oct. 2013).
[39] PCI, *DSS Requirements and Security Assessment Procedures, v3.0* (Nov. 2013).

annually and after significant change to the environment, and the responsibility for DSS requirements done respectively by service providers and the entity.

Thomas J. Shaw, Esq. *is an attorney at law, CPA, CRISC, CIP, CIPP, CISM, ERM^{P}, CISA, CGEIT and CCSK and author of the 2014 book* World War I Law and Lawyers – Issues, Cases, and Characters*, author of the 2013 book* Cloud Computing for Lawyers and Executives - A Global Approach, Second edition*, author of the 2013 book* World War II Law and Lawyers – Issues, Cases, and Characters*, author of the 2012 book* Children and the Internet – A Global Guide for Lawyers and Parents*, author of the 2011 book* Cloud Computing for Lawyers and Executives – A Global Approach *and editor/lead author of the committee's 2011 book,* Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*, author of several forthcoming legal books, and editor of the* EDDE Journal *and this publication. He can be reached at thomas@tshawlaw.com.*

Editor's Message

With this new issue, we are starting the fifth year of publishing the *Information Security & Privacy News* (*ISPN*), covering the world of information security and privacy law and technology each quarter. In this issue, we feature articles from a diverse set of authors based around the world on varied legal subjects covering information security, privacy, and information technology. The first article is written by Patrice Lyons of the Corporation for National Research Initiatives, addressing the management of information in digital form. The second article is from committee vice-chair Martha Chemas, on privacy and the rights of individuals and groups. The third article is from Josiah Dykstra of the U.S. Department of Defense, writing about how to obtain digital evidence from the cloud. The final article describes many of the recent changes globally to information security, privacy, and technology statutes/regulations, caselaw, and standards in the second half of 2013 and end of the first half. Thank you to all of the authors.

The Information Security committee continues to be dynamic and its list of activities can be found in the announcements that periodically are sent to the listserv and on the committee website, whose link is listed on the first page of this publication. Descriptions of the committee's workshops, pre-RSA meetings, webinars, face-to-face meetings, and other educational and professional activities can be located on the committee's website and listserv distributions. The format of the website has recently been significantly revised. You will also find the prior issues of this publication there. Please join the committee and volunteer for one of its many activities if you have not already done so.

I continue to ask that you share your knowledge and experience with your fellow professionals by writing an article for this periodical. Our next issue (Spring 2014) will come out in March, 2014. There are many members who have not yet been able to share their experience and knowledge through publishing an article here but please consider doing so to widen the understanding of all of our readers. Every qualified submission meeting the requirements explained in the Author Guidelines will be published, so please feel free to submit your articles or ideas, even if you are not quite ready for final publication. The issue after Spring (Summer 2014) will be published in June 2014. Until then.