INFORMATION SECURITY & PRIVACY NEWS

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

SPRING 2014 VOLUME 5 ISSUE 2

World War I – Keeping Information Private

By Thomas Shaw

Exactly a century ago, the first global war began. World War 1 (WWI) was to have far-reaching impacts in many areas, including the law. As discussed in my latest book (World War I Law and Lawyers – Issues, Cases, and Characters), this included the legal disciplines of privacy law and its trade-off with freedom of expression during wartime. I briefly analyzed those topics in a recent article for the IAPP. The security aspects of controlling wartime information were interesting as well. Security was essential to protect communications sent by wired and wireless mediums, including telephones and the new wireless telegraphy. Not only were these transmission types used but also important messages were sent with runners, who may have been humans or may have been animal, including pigeons and dogs. On the Western front, a *Read more*

What is Privacy in the Information Age?

By Mari Frank

Science and Privacy: together they constitute twin conditions of freedom in the twentieth century" - Privacy law in the electronic age is rapidly changing while at the same time our privacy is diminishing. Historically, the development of privacy law derived originally from the Declaration of Independence when Thomas Jefferson wrote: ***"****We declare these truths to be self-evident - that all men are endowed by their Creator with inalienable rights: that among these are the rights to life, liberty, and the pursuit of happiness."* As we analyze our country's freedom, it is clear that without privacy we have no liberty. Later, in 1791, when the Fourth Amendment to the U.S. Constitution was adopted, the notion of privacy was expanded to include *Read more*

The New Face of Brazilian Democracy vs. Technology

By Renato Opice Blum

The Constitution of the Federal Republic of Brazil, promulgated in 1988 begins; "all power emanates from the people, who exercise it through their representatives." A governance model of representative democracy has been established by the constitution and statute, the effectiveness of which is achieved through universal suffrage. The Constitution provides limited forms of direct participation by the people by way of plebiscite, referendum or popular initiative (art. 14-CF). However, the significant bureaucratic obstacles to such forms of direct participation have resulted in, today, such forms having become far removed from the everyday reality of Brazilian politics. Over the years citizens appear to have become accustomed to *Read more*

2014 (1Q) Information Law Updates: Cases, Statutes, and Standards

By Thomas Shaw

In the first quarter of 2014 and the end of 2013, 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*

World War I – Keeping Information Private

By Thomas Shaw

*Exactly a century ago, the first global war began. World War 1 (WWI) was to have far-reaching impacts in many areas, including the law. As discussed in my latest book (*World War I Law and Lawyers – Issues, Cases, and Characters*), this included the legal disciplines of privacy law and its trade-off with freedom of expression during wartime. I briefly analyzed those topics in a recent article for the IAPP. The security aspects of controlling wartime information were interesting as well. Security was essential to protect communications sent by wired and wireless mediums, including telephones and the new wireless telegraphy. Not only were these transmission types used but also important messages were sent with runners, who may have been humans or may have been animal, including pigeons and dogs. On the Western front, a* stalemate had arisen and trenches had been thrown up Belgium and France, spanning a transverse bisection of Western Europe. There needed to be a form of safe communication between those in the front lines, including troops, spotters, and sentries, and the artillery, reserves, and senior commanders towards the rear, plus also horizontally across the vast expanse trench works, to coordinate movements, shelling, and rotations.

Part of what was developed where known as trench codes. These cryptographic codes could be utilized because of the static conditions prevailing in the war in the west, despite the need for code books and their frequent replacement. Ciphers were a more common form of cryptography for armies on the move receiving wireless messages, using a cipher key but were subject to being broken. The trench codes, used by all the major armies, evolved to being three-character, two-step codes that were sufficiently secure, assuming both that the code books could be kept secure from raiding parties and that those engaged in combat conditions could be counted on to utilize them properly.

Although trench codes were initially developed to help secure telephone calls, these proved unwieldy and it was an introduction of a new technique by the American military late in the war that proved an unbreakable system for wireless voice calls. This was a system that used the Native American languages, specifically that of the Choctaw peoples. These languages had been passed down orally among the tribes, never having been written and as such, Central Power code breakers had nothing to refer to in trying to break these codes. This idea was resurrected in WWII, with the Navajo code talkers.

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.*

What is Privacy in the Information Age?

By Mari Frank

"Science and Privacy: together they constitute twin conditions of freedom in the twentieth century" - Dr. Alan Westin, (1929 – 2013) Professor of law Columbia University, Author, *Privacy and Freedom,* publisher, *Privacy & American Business*

Privacy law in the electronic age is rapidly changing while at the same time our privacy is diminishing. Historically, the development of privacy law derived originally from the Declaration of Independence when Thomas Jefferson wrote: ***"****We declare these truths to be self-evident - that all men are endowed by their Creator with inalienable rights: that among these are the rights to life, liberty, and the pursuit of happiness."* As we analyze our country's freedom, it is clear that without privacy we have no liberty.

Later, in 1791, when the Fourth Amendment to the U.S. Constitution was adopted, the notion of privacy was expanded to include "***the right of people to be secure in their persons, house, papers, and effects against unreasonable searches and seizures shall not be violated….***" Although the Fourth Amendment usually applies to governmental intrusion and criminal law, the intent of this provision, as our society's heritage, implies that all of us, whether or not criminals, nation should have a right to privacy in our ***personal effects.*** In the Information Age, shouldn't we also have this protection in our personal electronic information, our digital person in the surveillance society, and our on-line papers which also comprise our personal effects?

The Right to Privacy by Warren and Brandeis

"Privacy is the right to be alone--the most comprehensive of rights, and the right most valued by civilized man." — Louis D. Brandeis, Associate Justice, U.S. Supreme Court 1916 to 1939.

In 1890 Boston law firm partners Samuel Warren and Louis Brandeis wrote the famous Harvard Law Review article **The Right To Privacy** (4 Harv. L. Rev 193). They defined the right to privacy as ***the right to be let alone***. But they further explained that it signifies the right to choose **whether or not to share information about our** "private life, habits, acts and relations." With the invention of cameras and photography, information privacy about one's lifestyle, habits, and preferences were deemed an important valued right.

Brandeis and Warren considered privacy to be a right of psychological security determined by a person's **control** over what he or she wished to reveal or not disclose. They stated it was critical to recognize a right of privacy because when *information about an individual's private life is made*

available to others it tends to distort and injure that persons' sense of who he or she is. Our integrity and personal security is safeguarded by not having private information shared with others without our prior consent.

Privacy As It Relates To Our Nation's Freedom and Liberty

Warren and Brandeis considered privacy *essential to individualism.* They suggested that there must be legal remedies for privacy violations which should include tort damages, injunctive relief, and in some cases criminal prosecution. They hoped that legal remedies would be a deterrent to prevent intrusion into one's personal life By setting forth legal standards they surmised it would empower individuals to have more **control over their personal information.** Louis Brandeis (who later served as a Supreme Court Justice on the U.S. Supreme Court from 1916 to 1939,) greatly influenced the emergence of the right of privacy in the U.S. Constitution, several state constitutions, and tort law.

The Right of Privacy in the U.S. Constitution

"The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual." — Earl Warren, former Chief Justice US Supreme Court, (1953–1969) 30th *Governor of California*.

Although the U.S. Constitution doesn't specifically use the word "privacy," many Supreme Court cases have used the word "privacy" when interpreting the U.S. Constitution. In *Griswold v. Connecticut* (1965) 381 US 479 14 Led2d 510, 85 S CT 1678, the Supreme Court overturned a law prohibiting contraceptives based on privacy. The "zone of privacy" theory, for governmental purposes created as a result of the Fourth Amendment, became an important privacy right at the national level. Other critical privacy cases at the federal level were *Pierce v. Society of Sisters* (1925), 268 U.S.510,535 [child rearing and education] *Prince v. Massachusetts* (1944), 321 U.S. 158,166[family relationships]; *National Association for the Advancement of Colored People v. Alabama*, (1958) 357 U.S.449 (associations);*Roe v. Wade* (l973), 268 U.S.510,535 (abortion) ;*Loving v. Virginia* (1967), 388 U.S. 1,12 [marriage]; *Eisenstaedt v. Baird* (1972), 405 U.S. 438, 453-54 [sexual relations and contraception]

Invasion of Privacy in California

Before Privacy was Added to the California Constitution

An early case of privacy law in California was *Melvin v. Reid*, 297 P. 91 (Cal. App. 1931). In 1918, the court recognized a privacy action by a reformed prostitute against a movie which told the story of her earlier life (using her real maiden name) as a sex worker who was acquitted of murder. At that time there was no right of privacy tort, and the California constitution had not yet included "privacy" as a specific right. In that case the court found a *special right of privacy* by citing the California Constitution's notion of freedom at that time, "**life, liberty, and pursuing happiness." *"The right to***

pursue and obtain happiness is guaranteed to all by the fundamental law of our state. This right by its very nature includes the right to live free from the unwarranted attack of others upon one's liberty, property, and reputation."

In 1952, in the case of **Gill v. Curtis Publishing Company** (38 C2d 273, 278, 239 P2nd 630), the California Supreme Court cited **Melvin v. Reid** and upheld the common law tort of invasion of privacy which Brandeis and Samuels had described. The Gill court described the privacy right as *"The right to live one's life in seclusion, without being subjected to unwarranted and undesired publicity. In short it is the right to be let alone" (emphasis added).* (38 Cal.2d at 276).

Prosser's Categories of Privacy Torts

In 1960, William Prosser analyzed the law of privacy and tried to synthesize and create a taxonomy of privacy torts. He attempted to narrow the elements of privacy harms from the writings of Samuels and Brandeis to creating a categorization of four torts. (See William L. Prosser, Privacy, 48 CAL. L. REV 383, 389, 1960). The Restatement of Torts 2nd incorporated these torts:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness

These four areas of torts are quite specific and were developed many years before the invention of the Internet, big data, and wireless mobile devises. The torts are rather limiting as to information privacy because they don't address many of the privacy harms we face in the Information Age. For example they do not speak to the vast hidden collection, use, and dissemination of personal information that is bought, sold and shared with millions of computer databases, websites, social media, other wireless devices or blogs. Additionally the torts don't deal with how today anybody has the power to broadcast as a "journalist" information about us, or how we can be surveilled surreptitiously and exposed to a worldwide audience.. The collection of little bits of personal data about our lifestyle, our habits, our likes and dislikes, our family and more are gathered from various data sources and combined into hidden databases by various data brokers. This information is shared and sold many times over without our knowledge or consent. From their writings, it appears that Samuels and Brandeis would have found a privacy invasion in these situations using their common law approach. Unfortunately Prosser's narrow focused torts are not up to speed with the digital privacy violations that we are faced with today. Other ways of looking at privacy, however, provide guidance as to information privacy. California's (and four other states) Constitution specifically articulates privacy as a right and provides a stronger and broader based approach which includes data privacy.

Right to Privacy Added To the California Constitution In 1972

The California Constitution, Article 1 Declaration of Rights, Section I specifically states as follows:

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy (emphasis added).

Our California Constitutional right to privacy is specifically defined and far broader than the U.S. Constitution's right to privacy. The right extends to recovery from private parties as well as to governmental entities. For example in *White v. Davis* (1975) 13 C3d 757, 775, 120 CR 94), the court found that the California Constitutional right of privacy protects against the secret gathering of **information** about a person, and overbroad collection and retention of sensitive information.

The California Constitutional right of privacy was more clearly defined in *Hill v. National Collegiate Athletic Ass'n* (1994) 7 Cal.4th 1, 26 CR2d 834 with two basic privacy interests:

1. The interest of precluding the dissemination or misuse of confidential information (informational privacy). This is one of the hallmarks of the Fair Information Principles.

2. The interest in making personal decision or conducting personal activities without observation, intrusion, or interference (autonomy privacy). This relates back to the right to be let alone.

When we speak of information privacy, the Hill court analyzed whether there is a zone of privacy and whether the information shared or disclosed is considered private according to the society's norms." *A particular class of information is private when well-established social norms recognize the need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity. Such norms create a threshold reasonable expectation of privacy in the data at issue.*" (Hill v. National Collegiate Athletic Ass'n (1994) 7 Cal.4th 1, 26 CR2d 834).

So in the Information Age, the first question to ask in determining a privacy invasion is whether there is a zone of privacy or a reasonable expectation of privacy with regard to some allegation of privacy harm? An individual claiming a violation of a privacy right must possess a reasonable expectation of privacy under the particular circumstances, societal customs, practices, and physical settings surrounding the alleged invasion.

In our rapidly evolving technological age, the swiftly changing nature of widely accepted community norms may create or inhibit reasonable expectations of privacy. So for example if the person complaining voluntarily gives up information in a social media setting, does he have a right to complain if his future employer uses it? Or if a customer gives his information on a survey to get some benefit from that company, has he given up his privacy for that company to sell his information without prior explicit consent? Those who share in chatrooms or online forums may believe they have an

expectation of privacy only to learn that the information posted can be seen and captured by myriad third parties and used in ways that the person never would have consented to had he known the possibility of the use.

According to the Hill case, the next question to ask is if there is a serious invasion of privacy. It must be an outlandish breach of the current social norms. The privacy invasion "must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." The very act of freely sharing with friends on the web may in itself diminish the seriousness of the invasion if most others have no expectation of privacy.

Lastly, the Hill court suggested that the competing interests and their respective strengths or importance to the parties and to society need to be balanced. So we must ask, is there a compelling public need for disclosure of the data compared against the fundamental right to privacy?

The Hill court rehabilitated the common law view of privacy proposed by Brandeis and Samuels because the four elements of the tort of privacy did not suffice as to information privacy.

Information Privacy in the Electronic Age- Fair Information Principles

Dr. Alan F. Westin, (1929 – 2013) the "father" of present day information privacy was the long time law professor at Columbia University and renown as one of the premier experts on information privacy (Listen to my radio interview with him on Privacy Piracy archived at August 8, 2008, (www.kuci.org/privacypiracy). In his famous book, **Privacy and Freedom,** he defined privacy in this way:

"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

Dr. Westin explained "***Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communications of himself to others, in light of the environmental conditions and social norms set by the society in which he lives."***

Information or data privacy in the digital age refers to the evolving relationship between technology, security, and the right to privacy in the collection and sharing of data about ourselves. When personally identifiable information about individuals is collected, stored, accessed, acquired, and/or shared, there are concerns as to consent to collection, transparency of use, the ability to correct inaccurate records, the capability to stop unauthorized sharing, and the protection and security of sensitive and confidential records.

Congress and the Fair Information Practices Regarding Information Privacy

In order to safeguard privacy interests, Congress has enacted modern privacy statutes built around the "Fair Information Practices" framework that allocates rights and responsibilities in the collection and use of personal information. As a result of Dr. Westin's treatises, the concept of Fair Information Practices was first set out in the 1973 report: Records, Computers, and the Rights of Citizens. U.S. Department of Health, Education & Welfare: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (1973). The Code of Fair Information Practices describes basic informational privacy practices, such as:

- There must be no personal-data recordkeeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information obtained about him for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data, the promise of the data to be used for its intended use.
- All organizations collecting maintaining, using, sharing or disseminating such data must take reasonable precautions secure, protect and to prevent misuse of the data.

This privacy framework, whose inception can be traced back to Justice Brandeis, formed the basis of the US Privacy Act of 1974 and many US privacy laws such as the Fair Credit Reporting Act, which gives individuals the rights above with regard to know what credit information is being collected, how it is used, who it is shared with, and the right to dispute and correct such records, and the Health Insurance Portability and Accountability Act (HIPAA) which sets standards for privacy and disclosure of protected health information and permits review by patients and others and allows for a dispute mechanism for correcting records.

FAIR INFORMATION PRACTICES; THE CALIFORNIA ACT RELATING *ONLY* TO STATE GOVERNMENT AGENCIES

Just a few years after the US Privacy Act became law, California passed the Information Practices Act of 1977 (Civ. Code, § 1798 et seq.), which contains legislative findings that "(a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal

information and the lack of effective laws and legal remedies.(b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information... (c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits." (Civ. Code, § 1798.1.) Unfortunately, The US Privacy Act and the Information Practices Act apply only to governmental agencies and do not address the harms caused by private entities.

From a privacy perspective, it's unfortunate that both the federal US Privacy Act law and our state Information Practices Act are not comprehensive to include county and city government and private entities. The fundamental right of privacy in the electronic age demands that there be transparency as to the collection and use of our personal information. And to truly be a free society we should have the right to control and have the choice as to , how, when and with whom we share our personal information, We should also be assured that when the information is given, that the data be protected, secured, and used only for the purpose that we intended or authorize.

In our democratic and free society, privacy is one of the most cherished values as it is linked to our liberty. Our founding fathers fought for us to have the freedom to have privacy in our homes, in our religion, and in our private papers. Is there any one of us who does not deserve or want to have our privacy respected? As Justice Louis Brandeis first wrote and Columbia Law Professor Alan Westin reiterated, "***Privacy is an essential requirement for our human dignity."***

Mari Frank, mediator and Certified Information Privacy Professional (CIPP), is**,** co-author of Privacy Piracy, and author of *From Victim to Victor*: *A Step by Step Guide for Ending the Nightmare of Identity Theft; Safeguard Your Identity; The Complete Idiot's Guide to Recovering From Identity Theft; and Stepping Stones to Success.*. Since 2005, Mari has hosted the radio show *Privacy Piracy***,** KUCI 88.9 FM in Irvine (www.kuci.org/privacypiracy.) Mari has testified in Congress and the California Legislature, and serves as a qualified privacy expert in state and federal courts cases nationally. She's the Chair of the Privacy subcommittee of the LPMT Executive Committee of the State Bar of California, Board Member of the Privacy Rights Clearinghouse; and Fellow of the Ponemon Institute. www.marifrank.com; www.identitytheft.org; www.kuci.org/privacypiracy .

The New Face of Brazilian Democracy vs. Technology

By Renato Opice Blum

The Constitution of the Federal Republic of Brazil, promulgated in 1988 begins; "all power emanates from the people, who exercise it through their representatives." A governance model of representative democracy has been established by the constitution and statute, the effectiveness of which is achieved through universal suffrage.

The Constitution provides limited forms of direct participation by the people by way of plebiscite, referendum or popular initiative (art. 14-CF). However, the significant bureaucratic obstacles to such forms of direct participation have resulted in, today, such forms having become far removed from the everyday reality of Brazilian politics.

Over the years citizens appear to have become accustomed to participating in politics only through the electoral process. The responsibility of each voter being to choose a representative who, from that point onwards, is mandated to make decisions regarding policy in the federal bodies on their behalf. Thus, the role of the vast majority of Brazilians ends with the casting of their vote at the polls.

However, in recent years it appears that, in Brazil, technological development and the resulting growth of digital inclusion, notably through the popularity of social media, has allowed individuals to broaden their participation in the political life of the country, thus returning to them, power, influence that should have never relinquished given that the Constitution has always guaranteed their freedom of expression, of thought (section IV, art. 5 °-CF), including political thought, of course, within the limits of the law.

One might therefore consider that the somnolence of Brazilian people towards political affairs, apparent for many years, existed through a lack of tools, present today for example in social networks, which now provide opportunity to give scale to ideas and concerns, making it viable to share information between people with similar views that might live far from each other in what is a vast nation with many remote locations.

In fact the internet not only offers channels for the exchange of information and a possibility to mobilise society, which by the way caught politicians by surprise in recent months, but in fact also offers instruments to control and supervise the activities of the Three Powers, which have slowly forced a consolidation of electronic government, opening channels previously never accessible to the ordinary citizen. Pressure from the public led to legislation being passed to provide access to public information (Law 12.527/2011) which itself gave effect to subsection XXXIII of art. 5th-CF, that provides for the constitutional right to information. The legislation formalised that the state should guarantee

efficient access to information through agile, objective measures that are transparent, clear and in language that is easily understandable. In addition, public authorities must use all means and instruments to meet their obligation to "disclose through official sites on the world wide web" (internet).

The aim of Complementary Law 131/2009 is to impose transparency in public finances, so that today, applying the two laws, one can find online, amongst other things, official information regarding public accounts, salaries and contracting. Thus, the technology not only enables easier access to this important information, but also allows Brazilians to form their own opinions about it, to criticise and to share it, with the opportunity to ally themselves ideologically with other people interested in the topic.

It is also worth mentioning that the traditional media seems to have lost its monopoly on communication, with a veritable insurgency of amateur journalism by the public, highlighted in recent street demonstrations that attracted a massive audience on the web. The approach of these non-professionals was clearly more combative, but contributed in a different way to democracy, the internet providing objective, real content with a wide range of narrative.

It should however be noted that although these demonstrations and disruption through this virtual democracy is necessary in democratic society, there is of course a limit to them, the criminal law provides that people may and will be held accountable for their actions. There has been a crackdown on the crimes of slander, libel or defamation (Articles 138-140 of the Penal Code), published on Internet, which still apply, with a concrete possibility of increased punishment when such practices are directed against the President, Foreign Secretary or public officials, in relation to the execution of their duties (Article 141 of the Criminal Code).

Equally, those that either incite or condone criminal acts (Articles 286 and 287- CP) relating to damage, for example, aggravated when committed against public property, are also unacceptable and constitute criminal conduct and is punishable in through the same system as the socially repudiated suspects of corruption.

Thus, it is argued that in order that digital channels be utilised healthily in today´s democracy, that the process should play a fundamental role in informing and educating Brazilians who in turn will be able to more effectively exercise their rights and contribute to the growth of their nation.

Finally, it has long been said that ¨knowledge is power¨, it might be said that today's technology has helped the process of empowering, politically, the general public which gradually, with access to education and the ability to audit the government and then share through electronic tools has had the power "emanating from the people" which once slipped from their hands, restored, albeit subtly in a balanced way and absolutely in the best interest of the country.

Renato Opice Blum *- Attorney, Economist and President of the IT Advisory Board of Fecomercio.*

2014 (1Q) Information Law Updates: Cases, Statutes, and Standards

By Thomas Shaw

In the first quarter of 2014 and the end of 2013, 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.

HIPPA Privacy Rule, Mental Health and Lab Results[1]

HHS has released guidance on the HIPAA Privacy Rule in regards to mental health. The guidance addressed communications with a patient's family members, friends, or others involved in the patient's care; with family members when the patient is an adult; with the parent of a patient who is a minor; with family members, law enforcement, or others when the patient presents a serious and imminent threat of harm to self or others; and to law enforcement about the release of a patient brought in for an emergency psychiatric hold. It also gave considerations to the patient's capacity to agree or object to the sharing of their information; involving a patient's family members, friends, or others in dealing with patient failures to adhere to medication or other therapy; and listening to family members about their loved ones receiving mental health treatment. It also touches on topics such as intersection with others laws in a school environment, minor children's rights, such as access to psychotherapist's notes, and what doctors' privacy restrictions are if a patient might hurt themselves or others. HHS also issued a final rule amending prior rules to allow patients to get copies of their laboratory tests directly from

[1] HHS, HIPAA Privacy Rule and Sharing Information Related to Mental Health (Feb. 2014).

the labs instead of their medical provider, by modifying regulations under both HIPAA and the Clinical Laboratory Improvement Amendments of 1988.

Statutes and Regulations – International

South Africa Privacy Law[2]

The Republic of South Africa has a new privacy law. This purpose of this act is to give effect to the constitutional right of privacy, regulate the processing of personal information, give consumers rights and remedies for violations, and establish mechanisms to ensure compliance. The lawful processing of information includes: accountability, processing and further processing limitations, purpose specification, information quality, openness, security standards, and data subject participation. Special (sensitive) personal information or information on children may not be processed, subject to exceptions. An Information Regulator role is established, to educate, monitor, enforce, handle complaints, issue codes of conduct, and facilitate cross-border cooperation. Prior authorization is required for processing of unique identifiers, on criminal behavior, credit reporting or transferring special personal information or children's information to a third-party outside the country not providing adequate levels of protection. Direct marketing via unsolicited electronic communication and automated decision making are prohibited, subject to exceptions. Overseas transfers require the recipient to be subject to a law, binding agreement or corporate rules that providing for adequate levels of protection.

United Nations Right to Privacy[3]

The UN General Assembly passed a resolution regarding the right to privacy that tied those rights protected offline must also be protected online. This resolution reaffirmed the right to privacy in the Universal Declaration of Human Rights, recognized the global and open nature of the Internet and rapid advancement of ICT, affirmed that online people should have the right to privacy as they enjoy offline, and called on states to respect those rights, including reviewing mass surveillance practices and oversight practices. A report was requested of the UN High Commissioner for Human Rights on this topic.

Cases – Civil and Criminal

MOCA Systems v. Bernier[4]

This is another case invoking the CFAA, where the court looked to the meaning of that statute. The defendant was alleged to have taken the plaintiff's confidential information and trade secrets from their computer system to start his own firm. The court, recognizing the split among courts between how to interpret the "exceeds authorization" prong of the CFAA, determined that it did not need to

[2] South Africa, Protection of Personal Information Act, 2013 (Dec. 2013).
[3] UN, A/C.3/68/L.45/Rev.1, *Right to Privacy in the Digital Age* (Dec. 2013).
[4] *MOCA Systems, Inc. v. Bernier*, Case No. 13-10738 (D. Mass. Nov. 2013).

determine which of those two approaches was appropriate here, based on the facts. As the defendant was already terminated when he accessed the company's computer, his authorization had been clearly removed by the company. As such, his access was under the "without authorization" prong, not the "exceeds authorization" prong, and so the court ruled that the plaintiffs had stated a CFAA claim sufficient to withstand a motion to dismiss for failure to state a claim.

U.S v. Post[5]

In this child pornography case, the federal government used the metadata of a digital photograph taken of a young child and uploaded to the Internet to locate the perpetrator. Although the defendant admitted taking and uploading the pornographic photograph of the four-year-old child, he claimed in court a Fourth Amendment interest in the metadata of the photo that the government invaded. The government could not use the IP address, as the defendant had used an anonymous Internet connection. As the photo was taken with a smartphone, the GPS coordinates were included in the metadata. The defendant, a registered sex offender, admitted to no privacy interest in the uploaded photo but asked for suppression of it based on a retained privacy interest in the metadata. The court denied the suppression motion, finding that privacy interests in the photo could not be subdivided, drawing an analogy to the DNA on clothing left in a public place.

Cases – Regulatory

FTC and Goldenshores Technologies[6]

The FTC reached a settlement with Goldenshores Technologies, the maker of the Brightest Flashlight Free application for mobile phones. The complaint alleged deceptive business practices, in that the app developer was also transmitting to third parties the device's geolocation and device identifiers. This allowed tracking of users, all without their knowledge or consent. The marketing of the app did not disclose either the collection of this information or its dissemination to third parties, including advertisers. This is also not in the company's privacy policy and end-user license agreement. The app even collected data from the mobile device even before the end-user license agreement is accepted, giving the consumers "an illusory choice" about accepting these terms or not. The settlement agreement requires there be no misrepresentations of actual company practices regarding the collection and use of consumer information, that data collection practices be clearly spelled out in advance of collection, and then be done only with the express consent of the consumer.

HHS and Adult & Pediatric Dermatology[7]

The Department of Health and Human Services has reached a settlement with a dermatology clinic regarding violations of the HIPAA Privacy, Security, and Breach Notification Rules in regards to the theft of a thumb drive containing unsecured ePHI on over 2,000 patients. The Privacy Rule was violated by

[5] *United States v. Donald John Post St.*, Case No. 3:13-cr-00020 (S.D. Tex. Jan. 2014).
[6] *In the matter of Goldenshores Technologies, LLC*, FTC File No. 132 3087 (Dec. 2013).
[7] *In the matter of Adult & Pediatric Dermatology, P.C.*, HHS Cmplt. No. 12-133708 (Dec. 2013).

the disclosure of the information, the Security Rule by the lack of a risk and vulnerability assessment, and the Breach Notification Rule by the lack of written policies and training to respond to breaches. In addition to a Corrective Action Plan, the company is required to pay a fine of $150,000.

FTC and Accretive Health[8]

The FTC reached a settlement with hospital revenue cycle service provider Accretive Health regarding the theft of a laptop in 2011 containing patient information on over 20,000 patients. The complaint alleged that Accretive did not adequately control patient information from its own employees who did not currently require it, including using live data in employee training, and insecurely transporting such information, leading to the loss of patient data with the theft of the laptop. This is considered by the FTC to be an unfair business practice under the FTC Act. The failure to employ reasonable security practices is to be remedied through the implementation of a comprehensive infosec program.

FTC and Apple[9]

The FTC reached a settlement with Apple on mobile apps billing practices that allowed children to purchase virtual products without parental consent. These purchases were made because certain apps capture the parent's iTunes password and cache it for up to 15 minutes, during which time the child can purchase additional in-app virtual products, without additional parental consent. In addition, the in-app charging mechanism may not clearly differentiate which charges for various resources needed by games played by children are based on virtual currency or those that require real money. The FTC deemed these charges without informed parental consent to be unfair practices under the FTC Act. The settlement requires Apple to obtain express informed consent before applying in-app charges. Apple has allocated over $32 million to provide refunds to those consumers previously charged.

EU-U.S. Safe Harbor Certifications[10]

The FTC settled with a dozen companies who were claiming that they were certified under the U.S.-EU Safe Harbor framework and in three cases the U.S.-Swiss Safe Harbor framework when in fact their certifications had lapsed. The self-certification requires compliance with the safe harbor privacy principles to be able to transfer data from the EU to the U.S. The claim of certification is shown on websites or in privacy policies of the companies. The Commerce Department maintains a website showing which companies have re-certified or have not. The FTC then reached a settlement with a children's social network, Fantage, which in June 2012 did not renew its certification with Commerce, until January 2014. But at the same time, it did not modify its privacy policies showing this lack of certification, which constituted a deceptive trade practice under the FTC Act.

---

[8] *In the matter of Accretive Health, Inc.*, FTC File No. 122 3077 (Dec. 2013).
[9] *In the matter of Apple, Inc.*, FTC File No. 112-3108 (Jan. 2014).
[10] *In the matters of Apperian, Inc.; Atlanta Falcons Football Club, LLC; Baker Tilly Virchow Krause, LLP; BitTorrent, Inc.; Charles River Laboratories International, Inc.; DataMotion, Inc.; DDC Laboratories, Inc.; Level 3 Communications, LLC; PDB Sports, Ltd., d/b/a Denver Broncos Football Club; Reynolds Consumer Products Inc.; Receivable Management Services Corporation; and Tennessee Football, Inc.*, FTC File Nos. 142 3017-3020, 142 3022-3024, 142 3028, 142 3025, 142 3030-3032 (Jan. 2014); *In the matter of Fantage.com, Inc.*, FTC File No. 142 3026 (Feb. 2014).

FTC and LabMD[11]

The FTC rejected an appeal against it authority to oversee the data security practices of a company subject to HIPAA regulations. After being charged by the FTC with unfair business practices by not providing reasonable and adequate security for its business that included testing of patients and reporting to health care providers, the respondent filed a with a motion to dismiss. This motion included challenges to the FTC's power to regulate data security practices under the FTC Act (refuted by the FTC citing not only the commission's use of its deception and unfair practices prongs but going back to the authority provided under the 1914 act and never withdrawn by Congress, among other arguments). The respondent also challenged the ability of the FTC to regulate the data security practices of covered entities under HIPAA, which the commissioners also unanimously rejected, as there was no explicit rejection of its authority in any statutes including HIPAA that restricted the commissions' ability to enforce the FTC Act, including data security. The commission also rejected a due process challenge, based on the lack of data security regulations promulgated by the FTC.

FTC and GMR Transcription[12]

The FTC reached a settlement with a transcription services company for not protecting the personal information of consumers contained originally in the audio files being transcribed. This information included: names, dates of birth, addresses, email addresses, telephone numbers, Social Security numbers, driver's license numbers, tax information, medical histories, health care providers' examination notes, medications, and psychiatric notes. The alleged lack of reasonable security procedures included not requiring independent contractor typist to install antivirus software or subcontractors to use encryption or authentication or to monitor the subcontractor. This was contrary to their marketing materials and privacy policy, constituting unfair and deceptive trade practices. Inter alia the settlement requires periodic third-party assessments by security certified professionals.

California v. Kaiser Health[13]

The attorney general of California has filed suit against Kaiser Health, in regards to delayed notification of a data breach. In September 2011, the company learned that an unencrypted drive containing SSNs and other personal information of more than 20,000 Kaiser employees had been sold. It recovered the drive in December and analyzed it through February 2012. It was not until March 2012 that it began notifying those affected by the data breach. The state alleges that Kaiser engaged in unfair competition by both delaying notification for several months and also by making the unencrypted drive available to the public.

---

[11] *In the matter of Lab MD, Inc.*, FTC Docket No. 9357 (Jan. 2014).
[12] *In the matter of GMR Transcription Services, Inc.*, FTC File No. 122 3095 (Jan. 2014).
[13] *State of California v. Kaiser Foundation Health Plan*, Case No. RG14711370 (Sup. Ct. Cal. Jan. 2014).

FTC and TeleCheck[14]

The FTC reached a settlement with TeleCheck, a consumer reporting agency, for violations of the FCRA. The complaint alleged that the company did not reinvestigate disputed information that led to a consumer's check being refused. In the course of investigations, the company allegedly does not follow FCRA requirements for conducting investigations, timeliness in a number of areas, for updating consumer's files, for ensuring that the information does not reappear in the files, or for maintaining the accuracy of its information on individuals. Its affiliate also did not follow rules for furnishers of such information to others regarding information accuracy and integrity, as required by the Furnisher Rule. The company agreed to pay $3.5m to settle this suit.

Standards and Guidelines

GAO Report on Information Resellers[15]

General Accounting Office has released a report looking at the gaps in the current U.S. regulatory environment, especially in light of recent changes in technology and business practices for collecting and selling consumer information. Among the points made include that contrary to the long-standing Fair Information Privacy Principles, U.S. federal law does not provide a comprehensive way for consumers to control their personal information that is used by information resellers. This includes the ability to determine which information is held about individuals and by whom, to control their information (outside FRCA and GLBA), to correct it, the collection methods, types, and sources, online tracking or mobile technologies.

FFIEC Social Media Guidance[16]

The Federal Financial Institutions Examination Council released a guidance document for the use of social media by financial institutions to help with their risk assessment procedures. This includes looking to the applicable laws and risks that use of social media can create and the risk management programs to oversee the use of social media, including employee training and monitoring of social media sites and third party relationships. Financial institutions should be able "to identify, measure, monitor and control risk" related to the use of social media. The components of the risk management program for social media are included, as are the areas of social media risk by regulation and statute, along with reputation and operational risk.

DoD Cybersecurity Rules for Contractors[17]

The Department of Defense has issued rules to reduce the risk in its supply chain, targeting unclassified controlled technical information, including computer software. This addresses how contractors are to

---

[14] *U.S. v. TeleCheck Services, Inc.*, Case No. 1:14-cv-00062 (D.D.C. Jan. 2014).

[15] GAO, *Information Resellers - Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace* (Sept. 2013).

[16] FFIEC, *Social Media: Consumer Compliance Risk Management Guidance* (Dec. 2013).

[17] DoD, 78 Fed. Reg. No. 222, *Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information* (Nov. 2013).

protect such information in their systems from unauthorized access and disclosure and to report cyber intrusion events. To perform the former, contractors are directed to the current revision of NIST SP 800-53 controls as a base reference and to perform the latter, are required to notify the DoD within 72 hours of such a cyber intrusion incident.

GSA and DoD Recommendations[18]

In response to a presidential executive order, no. 13868, the General Services Administration and the Department of Defense have produced a report that attempts to align the cybersecurity risk management and acquisitions processes. To do so, it provides six major recommendations: Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions; Address cybersecurity in relevant training; Develop common cybersecurity definitions for federal acquisitions; Institute a federal acquisition cyber risk management strategy; Include a requirement to purchase from original equipment or component manufacturers, their authorized resellers, or other trusted sources, for appropriate acquisitions; and Increase government accountability for cyber risk management.

NIST Cybersecurity Framework[19]

NIST has released version 1.0 of its framework for assisting the critical infrastructure industry in addressing their cybersecurity risks. This voluntary, non-regulatory framework was created as a "set of industry standards and best practices" from a collaboration between the private and public sectors. It contains three parts, the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Core is the industry standards, guidelines, and practices viewed through five functions: Identify, Protect, Detect, Respond, and Recover, that are in turn broken into categories and subcategories. The Tiers provide four levels from Partial to Risk Informed to Repeatable to Adaptive that each address the risk management process, the integrated risk management program, and external participation. The Profile provides the ability to create a current and target critical infrastructure cybersecurity risk posture from the functions, categories, and subcategories.

Online Privacy for Students[20]

The Department of Education's Privacy Technical Assistance Center has issued guidance to help schools and teachers interpret the applicable federal laws and to implement best practices to protect students online. Specially, the guidance looks at security and private considerations for third-party mobile apps, web-based tools, and computer software supporting the education provided by schools and school systems accessed over the Internet. Examples include the disclosure of student personally identifiable information to service providers and what they can do with that information. Also, the American Legislative Exchange Council recently provided a model bill (the Student Data Accessibility, Transparency, and Accountability Act) for state legislatures for student privacy that included requiring

[18] GSA/DoD, *Improving Cybersecurity and Resilience through Acquisition* (Nov. 2013).
[19] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 2014).
[20] Dept. of Educ. PTAC, *Protecting Student Privacy while Using Online Educational Services* (Feb. 2014).

data security plans, disclosing the data points collected on students, requiring privacy and security provisions in vendor contracts, and the appointment of chief privacy officers.

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 well into the fifth year of publishing the *Information Security & Privacy News* (*ISPN*), covering the world of information security, privacy, and cloud computing 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, cloud computing, and information technology. The first article describes some issues related to the security needs of the military in World War I starting one hundred years ago. The second article is by well-known privacy advocate Mari Frank, on what privacy means in the Information Age. The third article is from frequent contributor Renato Opice Blum of IT Advisory Board of Fecomercio, writing about democracy versus technology in Brazil. The final article describes many of the recent changes globally to information security, privacy, cloud computing and technology statutes/regulations, caselaw, and standards in the first quarter of 2014 and end of 2013. 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 (Summer 2014) will come out in June, 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 Summer (Autumn 2014) will be published in September 2014. Until then.