

INFORMATION SECURITY & PRIVACY NEWS

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

SPRING 2011 VOLUME 2 ISSUE 2

Editor

[Thomas J Shaw, Esq.](#)
Tokyo, Japan

Committee Leadership

Co-Chairs' Message

Co-Chairs:

[David J Navetta](#)
Denver, CO

[Kathryn R. Coburn](#)
Pacific Palisades, CA

Vice-Chairs:

[Benjamin Tomhave](#)
Fairfax, VA

[Peter McLaughlin](#)
Boston, MA

[SciTech Homepage](#)

[InfoSec Homepage](#)

[Join the InfoSec
Committee](#)

© 2011 American Bar Association. All rights reserved. Editorial policy: *Information Security & Privacy News* endeavors to provide information about current developments in law, information security, privacy and technology that is of professional interest to the members of the Information Security Committee of the ABA Section of Science & Technology Law. Material published in *Information Security & Privacy News* reflect the views of the authors and does not necessarily reflect the position of the ABA, the Section of Science & Technology Law, or the Editor(s).



ABA SECTION OF
SCIENCE & TECHNOLOGY LAW

Book Extract: *Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*

By [Thomas Shaw](#)

This month, our committee's new book, *Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*, will become available ([here](#)). The ABA bookstore's webpage shows the table of contents, all of the contributors and part of the first chapter. But I wanted to do more to give a flavor for what is inside, so the following are a series of brief extracts from the book. In creating a book with such a (very) large number of contributors, most if not all of whose work was intertwined with the work of others, it is not possible to individually credit each author's writing in each section. As such, I am using this article as a way to credit some of those contributors whose writings truly excelled. [Read more](#)

Social Networking: Open Discovery Versus Privacy and the Battle Between the Coasts

By [Bradley J. Schaufenbuel](#)

Do Facebook and MySpace users have a reasonable expectation of privacy in their non-public posts? Are private communications sent within a social network site discoverable in a civil action? This paper explores the struggle that courts have had in balancing privacy interests and open discovery in the context of social networking sites. Part I discusses the existing legal framework, including procedural rules, statutes, and case law that are pertinent to the topic. Part II analyses the issue in depth, arguing that although individuals have a reasonable expectation of privacy in their non-public social networking activities, these communications should [Read more](#)

National Security Officials Want Enhanced Capability to Intercept Communications Over the Internet

By [Kathryn R. Coburn](#)

Businesses that provide Internet Services can look for new government regulations in 2011. At a meeting of law enforcement officials in October 2010, FBI Director Robert Mueller warned the audience of the growing role of the Internet as a tool in spreading terrorism. In the words of Director Mueller, "The Internet has become a facilitator-even an accelerant- for terrorist and criminal activity." He emphasized the importance of technology in meeting that threat through the use of searchable databases that find connections and patterns in the information [Read more](#)

Knocking on the Cloud's Door - Obligations of Cloud Service Providers to Maintain the Privacy of Information Entrusted to Them

By [Yakov Ginzburg](#)

When asked whether users should be sharing information with Google as if it were a "trusted friend," Eric Schmidt, then-CEO of Google, Inc. (one of the major cloud service providers), responded, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." Such cavalier attitude toward privacy from the head of a major cloud provider is very surprising. While criminals, terrorists, and social deviants may use the Cloud to achieve their illicit goals, the Cloud is mainly used for legitimate purposes. [Read more](#)

Book Extract: *Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*

By Thomas Shaw



This month, our committee's new book, *Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*, will become available ([here](#)). The ABA bookstore's webpage shows the table of contents, all of the contributors and part of the first chapter. But I wanted to do more to give a flavor for what is inside, so the following are a series of brief extracts from the book. In creating a book with such a (very) large number of contributors, most if not all of whose work was intertwined with the work of others, it is not possible to individually credit each author's writing in each section. As such, I am using this article as a way to credit and give face to some of those contributors whose writings truly excelled.

Now that the book is published, here are some ways to get it promoted. The book will be reviewed in the upcoming issue of *SciTech Lawyer*. We are also having a number of testimonials written on the book. There is a whole marketing plan around the book's publication, including an upcoming press release. There are also a variety of non-traditional marketing efforts underway to widely disseminate the book, including blurbs by presenters at the RSA conference and availability in the RSA bookstore, outreach to non-lawyer organizations and contacts with foreign bar associations. Please feel free to recommend this book to colleagues and clients and add it to your professional networks and presentations. Congratulations to all of you who wrote so well and thank you all for your team work.

I also wanted to thank here not only those who followed through on their authoring commitments but several others who agreed to step into the breach when the original authors could not meet those commitments. Leading this group is Charlene Brownlee, who stepped in to help not just once but twice. Also stepping in and accepting the call to pick up the baton were Edward R. McNicholas, Rebecca Grassl Bradley, Daniel Garrie, Benjamin Tomhave, Dan Oseran and Steven Teppler. Your assistance in this complex endeavor is very much appreciated and made the book so much the better.

The Extracts – Introductory Paragraphs

Encryption – Robert Jueneman
(in Chapter 5)



The need for encryption has increased parallel to the increased movement of data outside controlled environments. The use of the Internet in all its forms, the vast increase in the use of outsourcing, and many new types of mobile technology mean that an organization's data may need to be protected at all times in all locations. Several key questions must be addressed in creating a cryptographic system that deploys encryption:

- How sensitive is my information, and which encryption algorithms and key lengths are recommended to protect it?
- What is the difference between data at rest, data in transit, and data in use, and what should be done to protect this data?
- What are the key business, information security, and privacy risks, and what can be done to mitigate them?

Canadian Information Security and Privacy Law – Michael Power

(in Chapter 2)



Canada is a federal state with a number of data protection laws governing the processing of personal information. Comprehensive legislation, for private-sector organizations, exists in the form of the federal Personal Information Protection and Electronic Documents Act (PIPEDA), as well as provincial statutes in British Columbia, Alberta, and Quebec. Determining which laws apply requires an analysis of a number of factors, but PIPEDA contains a mechanism to avoid duplicate coverage by exempting organizations already subject to “substantially similar” provincial legislation.”

Health Insurance Portability and Accountability Act / Health Information Technology for Economic and Clinical Health Act – Charlene Brownlee

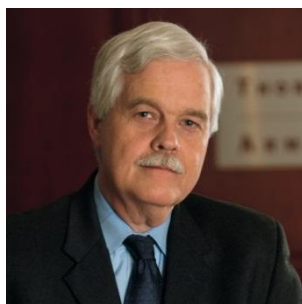
(in Chapter 2)



To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) included Administrative Simplification provisions that required the Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. The Office for Civil Rights (OCR) administers and enforces the Privacy Rule and Security Rule. The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules.

Safeguarding Client Data: Lawyer’s Ethical and Legal Obligations – David Ries

(in Chapter 2)



Confidential data in computers and information systems, including those used by lawyers and law firms, faces greater security threats today than ever before. Lawyers have ethical, common law, and statutory obligations to protect information relating to clients. In addition, protection of confidential information is sound business and professional practice. It is critical for

attorneys to understand and address these obligations and to exercise constant vigilance to protect client data.

Identity Management and Authorization - Tom Smedinghoff

(in Chapter 5)



In this age of the Internet, social networks, and mobile computing and the related issues of phishing, hacking, social engineering, and identity theft discussed in Chapter 4, the answer to the question, "who are you?" becomes critical. On the Internet, without the benefit of face-to-face personal contact, authenticating the identity of the remote party is of the utmost importance. It plays a key role in fighting identity fraud, is essential to establishing the trust necessary to facilitate electronic transactions of all types, and in many cases has become a legal obligation.

FTC Regulatory Actions – Marcia Hofmann

(in Chapter 3)



The Federal Trade Commission (FTC or the Commission) is the federal agency tasked with ensuring the efficient operation of the marketplace by protecting consumers from unfair and deceptive trade practices and promoting competition among businesses. While the FTC enforces various antitrust and consumer protection laws, this section discusses the Commission's enforcement of the Federal Trade Commission Act (FTCA) and other statutes designed to protect the privacy of consumer information.

Data security is one of the top priorities under the FTC's privacy agenda. The FTC is also responsible for coordinating the federal response to identity theft and assistance for victims of identity theft.

Contract-based Claims – David Navetta

(in Chapter 3)



Information technology and the processing, storage, and transmission of information are ubiquitous. At the same time (and likely as a result of this ubiquity), the regulatory and legal liability environments pose increased risks and potential for enormous liability. Additionally, whether with cloud computing providers or via more traditional avenues for outsourcing information technology functions (e.g., ASP, hosting, and storage), companies are increasingly outsourcing their information technology functions to third-

party service providers to stay competitive and efficient. It is likely that adoption of these practices will continue to increase.

The Need to Verify Certificate Authorities – Steven Roosa (in Chapter 5)



Secure business communications rely on the PKI model described in the previous section. This process involves the authentication of the parties involved in the communication by third party Certificate Authorities (CAs). While some CAs may be well-known and easily trusted, others may be unknown or may involve CAs that organizations may not want to be part of their network of trust for secure communications. As such, it is necessary for lawyers and technologists to work together to actively determine all of the CAs that the organization will trust, instead of passively accepting that all CAs are worthy of trust. This starts with understanding the models of trust used by end-user Internet browsers when accessing websites.

Relationship Between Information Security and Privacy – Tanya Forsheit (in Chapter 1)



Several relationships exist between information security and privacy. One relationship of information security and privacy is that one enables the other. Privacy requires information security to achieve its objectives. At the same time, privacy is larger than just the information security controls designed and implemented on its behalf. There are many other aspects to privacy that are not part of what information security aims to achieve. To understand this difference, we must first define privacy before looking at its relationships with information security.

The Role of Lawyers – E. Regan Adams (in Chapter 8)



Lawyers play a crucial role in assisting an organization to implement information security and privacy policies and practices. The modern lawyer plays an ever more interesting and vital role—one undergoing transformation as digitalization sweeps the globe and the dynamic nature of data rapidly changes how organizations function. Today, the lawyer's job is no longer constrained to knowing just the law; it is about knowing processes and technology and shaping them to comply with laws and regulations in all subject areas and locations. Two of the lawyer's most critical roles are to manage risk and to help build defensibility into the core of an organization's information security and privacy practices.

Social Networking: Open Discovery Versus Privacy and the Battle Between the Coasts

By *Bradley J. Schaufenbuel*



Do Facebook and MySpace users have a reasonable expectation of privacy in their non-public posts? Are private communications sent within a social network site discoverable in a civil action? This paper explores the struggle that courts have had in balancing privacy interests and open discovery in the context of social networking sites. Part I discusses the existing legal framework, including procedural rules, statutes, and case law that are pertinent to the topic. Part II analyzes the issue in depth, arguing that although individuals have a reasonable expectation of privacy in their non-public social networking activities, these communications should nevertheless be discoverable in civil litigation. Finally, Part III proposes that the Stored Communications Act (“SCA”) be amended to clarify its interaction with civil discovery rules.

Part I – Background

Existing Legal Framework

Scope of Civil Discovery

Unlike in civil law jurisdictions, the United States prefers broad and open discovery.¹ Any non-privileged information that is relevant to a claim in the dispute or that may lead thereto is generally discoverable.² The scope of what is discoverable is larger than the scope of what is ultimately admissible as evidence at trial.³ Furthermore, information that is filed with the court or utilized in judicial proceedings is, absent a protective order specifying otherwise, made a part of the public record.⁴ Information procured via discovery not covered by a protective order can also be disclosed directly to the public by the party that obtained it.⁵

Privilege

Privilege is the right to shield information, including documents, from discovery, no matter how important or relevant to the litigation.⁶ The attorney-client privilege, which excludes from discovery

¹ STEPHEN C. YEAZELL, CIVIL PROCEDURE 415 (7th ed. 2008).

² FED. R. CIV. P. 26(b)(1).

³ *Id.*

⁴ *San Jose Mercury News, Inc. v. United States Dist. Court N. Dist.*, 187 F.3d 1096, 1103 (9th Cir. 1999); *Phillips v. General Motors Corp.*, 307 F.3d 1206, 1210 (9th Cir. 2002); MICHAEL D. SCOTT, SCOTT ON INFORMATION TECHNOLOGY LAW § 6.17 (3d ed. Supp. 2008).

⁵ *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 37 (1984), available at http://scholar.google.com/scholar_case?case=13843985791078501976.

⁶ *Stalker v. Abraham*, 897 N.Y.S.2d 250, 253 (N.Y. App. Div. 2010), available at <http://decisions.courts.state.ny.us/ad3/Decisions/2010/506920.pdf>.

communications between a lawyer and his client related to the representation, is a classic example.⁷ The “privacy” of a litigant is not a privilege.⁸ Thus privacy does not normally prevent discovery by an opposing party.⁹ Privacy, for instance, is no excuse for destroying information to keep it out of a civil case.¹⁰

Protective Orders

If a privilege does not apply, a party may seek a protective order limiting the scope of discovery or the subsequent disclosure of information in the public record.¹¹ The court, however, will only issue such an order “to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense”.¹² Given the public policy preference for open discovery, courts generally construe this exception narrowly.¹³

Privacy’s Role in the Limitation of Civil Discovery

The privacy of a litigant is often weighed by the court as a factor in determining whether to issue a protective order, but not usually to prevent discovery altogether as with a privilege.¹⁴ Privacy interests normally justify only a protective order that limits the public disclosure of discoverable information.¹⁵ Thus relevant but “private” non-privileged information usually remains discoverable, even if its subsequent disclosures to anyone except the court and the parties to the litigation are limited by a protective order.¹⁶ Furthermore, if a litigant has previously made information available to the public, he or she cannot later object to its discoverability or subsequent disclosure.¹⁷

⁷ *Upjohn v. United States*, 449 U.S. 383, 389 (1981), available at http://scholar.google.com/scholar_case?case=5153750416071396937.

⁸ *Condit v. Dunne*, 225 F.R.D. 100, 107-08 (S.D.N.Y. 2004), available at http://www.firstamendmentcoalition.org/handbook/cases/Condit_v_Dunne.pdf. But see *Pearce v. Club Med Sales, Inc.*, 172 F.R.D. 407, 410 (N.D. Cal. 1997) (noting that California courts have extended the right to privacy to encompass a privilege justifying a litigant's refusal to answer intrusive deposition questions).

⁹ David K. Isom, *Romano and Facebook: Muddling Toward the Law of Privacy on Social Networks*, INFORMATION LAW GROUP (Oct. 12, 2010), <http://www.infolawgroup.com/2010/10/articles/social-networking/romano-and-facebook-muddling-toward-the-law-of-privacy-on-social-networks>.

¹⁰ *Leon v. IDX Systems Corp.*, 464 F. 3d 951, 959 (9th Cir. 2006), available at http://scholar.google.com/scholar_case?case=9241663656315436980.

¹¹ FED. R. CIV. P. 26(c).

¹² FED. R. CIV. P. 26(c)(1).

¹³ *Keith H. v. Long Beach Unified School Dist.*, 228 F.R.D. 652, 659 (C.D. Cal. 2005); *Loussier v. Universal Music Group, Inc.*, 214 F.R.D. 174, 177 (S.D.N.Y. 2003).

¹⁴ *Arnold v. Pennsylvania Dept. of Trans.*, 477 F.3d 105, 108 (3d Cir. 2007), available at http://scholar.google.com/scholar_case?case=8780753427374743390.

¹⁵ David Navetta, *The Law of Privacy on Social Networks*, INFOSEC ISLAND (Oct. 20, 2010), <https://www.infosecisland.com/blogview/8917-The-Law-of-Privacy-on-Social-Networks.html>.

¹⁶ Howard M. Erichson, *Court-Ordered Confidentiality in Discovery*, 81 CHI.-KENT L. REV. 357, 370 (2006), available at <http://www.cklawreview.com/wp-content/uploads/vol81no2/Erichson.pdf>.

¹⁷ Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 HARV. L. REV. 427, 464 (1991).

Fourth Amendment

The Fourth Amendment to the United States Constitution protects the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures".¹⁸ However, when applied to information stored online, the Fourth Amendment's protections are potentially far weaker.¹⁹ In part, this is because the Fourth Amendment defines the "right to be secure" in spatial terms that do not directly apply to the "reasonable expectation of privacy" in an online context.²⁰ In addition, society has not reached a clear consensus over expectations of privacy in terms of more modern forms of recorded and / or transmitted information.²¹ Furthermore, the Fourth Amendment generally does not apply to private civil litigants absent a finding of "state action".²²

Third Party Doctrine

Users generally entrust the security of online information to a third party (in this case, a social networking site).²³ In many cases, Fourth Amendment jurisprudence has held that, in so doing, users relinquish any expectation of privacy.²⁴ The so-called "third party doctrine" holds "...that knowingly revealing information to a third party relinquishes Fourth Amendment protection in that information".²⁵ While a search warrant and probable cause are required to search one's home, under the third party doctrine, only a subpoena and prior notice (a much lower hurdle than "probable cause") are needed to compel an Internet Service Provider ("ISP") to disclose the contents of an e-mail message or of files stored on a server.²⁶

¹⁸ U.S. CONST. amend. IV.

¹⁹ Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 *FORDHAM L. REV.* 349, 365 (2009), available at http://law.fordham.edu/assets/LawReview/Scolnik_October_2009.pdf.

²⁰ Donald L. Doernberg, "Can You Hear Me Now?": *Expectations of Privacy, False Friends, and the Perils of Speaking Under the Supreme Court's Fourth Amendment Jurisprudence*, 39 *IND. L. REV.* 253, 263 (2006), available at <http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1263&context=lawfaculty>.

²¹ Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 *MICH. TELECOMM. TECH. L. REV.* 61, 72 (2000), available at <http://www.mttl.org/volsix/skok.html>.

²² *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921), available at http://scholar.google.com/scholar_case?case=10755134066232305233. But see *Shelley v. Kramer*, 334 U.S. 1 (1948), available at http://scholar.google.com/scholar_case?case=12732018998507979172 (finding the use of the legal system by private parties to maintain impermissible discrimination via restrictive covenants to be "state action").

²³ PATRICIA L. BELLIA, PAUL SCHIFF BERMAN, & DAVID G. POST, *CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE* 481 (3d ed. 2007).

²⁴ *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring), available at http://scholar.google.com/scholar_case?case=9210492700696416594.

²⁵ Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 *MICH. L. REV.* 561, 561 (2009), available at <http://ssrn.com/abstract=1138128>.

²⁶ Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 *GEO. WASH. L. REV.* 1208 (2004), available at <http://ssrn.com/abstract=421860>.

The Stored Communications Act

The SCA is a statute that was enacted by the United States Congress in 1986.²⁷ It is not a stand-alone law but forms part of the Electronic Communications Privacy Act (“ECPA”).²⁸ The SCA addresses voluntary and compelled disclosure of “stored wire and electronic communications and transactional records” held by third-party online service providers.²⁹

The SCA creates Fourth Amendment-like privacy protection for e-mail and other digital communications stored on the Internet.³⁰ It prohibits the government from compelling an online service provider to turn over content and non-content information (such as logs and “envelope” information from e-mail messages) absent a court-issued warrant.³¹ In addition, and more important for the purposes of this paper, the SCA prohibits commercial online service providers from disclosing content information to nongovernment entities absent a statutorily defined exception.³²

The SCA and Civil Discovery

The SCA contains several exceptions to its general prohibition of disclosure to third parties.³³ Included are exceptions for disclosure to an addressee or the intended recipient of a communication,³⁴ to ISP employees related to the rendition of services,³⁵ and to a government agency in an emergency situation involving danger of death or serious bodily harm.³⁶ The privacy protections that are mandated under the SCA depend on whether an ISP is providing just electronic communications services (“ECS”) or also remote computing services (“RCS”).³⁷

Notably absent, however, is an exception for disclosure pursuant to a civil subpoena. Several courts have held that there is no “implied” civil subpoena exception to the SCA that permits the disclosure of the content of communications.³⁸ As a California court put it:

²⁷ Stored Communications Act, 18 U.S.C. §§ 2701- 2712 (2006), available at http://www.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_121.html.

²⁸ Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510 et seq.).

²⁹ Warshak v. United States, 490 F.3d 455, 462 (6th Cir. 2007), available at http://scholar.google.com/scholar_case?case=941624893598081483.

³⁰ Michael Gallo, *E-mail Privacy – Whether Court Order Disclosure of E-mail Content, per the Stored Communications Act, Violates the Fourth Amendment*, 26 MICH. IT LAWYER 11, 12 (2009), available at http://www.michbar.org/computer/pdfs/vol26_1.pdf.

³¹ Scolnik, *supra* note 19, at 382.

³² Timothy G. Ackermann, *Consent and Discovery Under the Stored Communications Act*, THE FEDERAL LAWYER, Nov. / Dec. 2009, at 42-43, available at http://www.pattersonsheridan.com/images/uploads/SCA_Control_article_PUBLISHED-crop.pdf.

³³ These exceptions are codified in 18 U.S.C. § 2702(b).

³⁴ 18 U.S.C. § 2702(b)(1).

³⁵ 18 U.S.C. § 2702(b)(5).

³⁶ 18 U.S.C. § 2702(b)(8).

³⁷ The term “Remote Computing Service” is defined in 18 U.S.C. § 2711(2).

³⁸ O’Grady v. Superior Court, 139 Cal. App. 4th 1423, 1443 (Cal. App. 6th Dist. 2006); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008); *Viacom International, Inc. v. YouTube, Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008).

Here there is no pertinent ambiguity in the language of the statute. It clearly prohibits any disclosure of stored e-mail, other than as authorized by enumerated exceptions. [The plaintiff] would apparently have us declare an implicit exception for civil discovery subpoenas. But by enacting a number of quite particular exceptions to the rule of non-disclosure, Congress demonstrated that it knew quite well how to make exceptions to that rule.³⁹

Social Networking Sites

To properly apply the law to the discovery of social networking site communications, it is necessary to possess a thorough understanding of this medium. There are generally three types of information found on social networking sites: 1) public information that is available to the general public, 2) semi-private information that the subscriber restricts to a self-selected group of friends, and 3) private one-to-one and one-to-many messages sent through the social networking site.⁴⁰ Most social networking sites permit users to select granular privacy settings that determine what communications are made available to whom.⁴¹

Case Law

Earlier Cases

Cases where the contents of a litigant's social networking site communications are sought as evidence in a civil matter are becoming more and more common.⁴² In most of these cases, social networking communications are requested by one party to expose litigant duplicity (i.e., arguing one thing in court but saying something contrary online) by the other party.⁴³ Two examples follow. In *Beye v. Horizon Blue Cross Blue Shield of New Jersey*, a father sued his health insurance company after the insurer refused to pay benefits for the treatment of his daughter for anorexia or bulimia.⁴⁴ The case turned on whether the girl's condition was the result of mental illness or was biologically based (New Jersey law requires coverage of mental illness only if it is biologically based).⁴⁵ Horizon claimed that the eating problems were not biologically based and that the girl's social networking communications could point to emotional causes.⁴⁶ The court ordered the plaintiff to produce the contents of the non-public

³⁹ *O'Grady*, 39 Cal. App. 4th at 1443.

⁴⁰ Joseph G. Poluka & Michelle Gitlitz Courtney, *Are Facebook Postings Discoverable?*, BLANK ROME LLP NEWSLETTER, Oct. 2010, at 2, available at <http://www.blankrome.com/pdf.cfm?contentID=37&itemID=2326>.

⁴¹ Stacie K. Linder, *Developing Facts Through the Internet and Social Networking Sites: Electronic Informal Investigation and Discovery*, Address to the 25th Annual Claims Handling Seminar (May 20, 2010), transcript available at http://www.heyloyster.com/data/files/Seminar_2010WC/2010_WC_D_SKL.pdf.

⁴² John S. Wilson, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1202 (2008), available at <http://www.law.uoregon.edu/org/olr/archives/86/Wilson.pdf>.

⁴³ Eric Goldman, *MySpace Postings Foil Another Litigant – Sedie v. U.S.*, GOLDMAN'S OBSERVATIONS (Apr. 28, 2010, 7:20 AM), http://blog.ericgoldman.org/personal/archives/2010/04/myspace_posting.html.

⁴⁴ *Beye v. Horizon Blue Cross Blue Shield of New Jersey*, No. 06-5337, 2008 WL 3064757 (D.N.J. Jul. 29, 2008), available at <http://www.provideradvocate.com/PDFs/July29.pdf>.

⁴⁵ John M. Grohol, *Think Social Networks, Blogs Can't Hurt You?*, WORLD OF PSYCHOLOGY (Feb. 2, 2008), <http://psychcentral.com/blog/archives/2008/02/02/think-social-networks-are-harmless-think-again>.

⁴⁶ Mary Pat Gallagher, *MySpace, Facebook Pages Called Key to Dispute Over Insurance Coverage for Eating Disorders*, N.J. L.J. (Feb. 1, 2008), <http://www.law.com/jsp/article.jsp?id=1201779829458>.

portions of the girl's Facebook and MySpace accounts, even if it reflected sensitive medical conditions, because of "the diminished expectation of privacy due to the posting and sharing of the information".⁴⁷

In *Ledbetter v. Wal-Mart Stores, Inc.*, a federal magistrate judge denied a motion for a protective order regarding subpoenas the defendants had issued to social networking sites.⁴⁸ The plaintiffs were seeking damages for alleged injuries arising out of an electrical accident at a Wal-Mart store.⁴⁹ Wal-Mart's attorneys discovered through Internet searches that the plaintiffs had posted information that related to and discounted their damage claims on the publicly available portions of social networking sites.⁵⁰ Wal-Mart subpoenaed information from the social networking sites regarding the private areas of the plaintiffs' accounts.⁵¹ The court rejected the plaintiffs' argument that their social networking account information was privileged and held that "the information sought within the four corners of the subpoenas issued to Facebook, MySpace, and Meetup.Com is reasonably calculated to lead to the discovery of admissible evidence a[nd] is relevant to the issues in this case".⁵²

In *Beye*, the defendant requested the social networking communications directly from the plaintiff via a Rule 34 request for production. It did not, however, attempt to subpoena the social networking sites themselves. In *Ledbetter*, on the other hand, the defendant did subpoena the social networking sites. However, neither the social networking sites involved nor the plaintiff raised the issue of whether compliance with the subpoena by the social networking sites violated the SCA. Thus the court applied the general law of civil discovery and ordered disclosure.

The legal landscape changed this year, when decisions were rendered in two civil cases in which either a social networking service provider or a party to the litigation raised the SCA in an objection to the subpoena of a social networking site. Two courts – a New York state court and a California federal court – came to very different (although not necessarily inconsistent) conclusions on the question of whether private social networking content should be disclosed for the purpose of civil discovery. Each case will be examined in turn.

⁴⁷ Andy Serwin, *ECPA Reform – Inconsistent Holdings on Social Media*, PRIVACY & SECURITY SOURCE (Oct. 2, 2010), <http://www.privacysecuritysource.com/ecpa-reform-inconsistent-holdings-on-social-media>.

⁴⁸ *Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009).

⁴⁹ *Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-cv-01958-WYD-MJW, 2009 WL 3837878, at *2. (D. Colo. Nov. 13, 2009), available at http://scholar.google.com/scholar_case?case=16083892536168446022.

⁵⁰ Shannon Awsumb, *Social Networking Sites: The Next E-Discovery Frontier*, 66 BENCH & BAR OF MINN. 22, 26 (Nov. 2009), available at <http://www.mnbar.org/benchandbar/2009/nov09/networking.html>.

⁵¹ Andrew C. Payne, *Twitigation: Old Rules in a New World*, 49 WASHBURN L.J. 841, 861 (2010), available at <http://www.washburnlaw.edu/wlj/49-3/articles/payne-andrew.pdf>.

⁵² John J. Cord & Robert K. Jenner, *Social Networking Websites: How to Reap the Benefits and Avoid the Hazards, Part II*, TRIAL REPORTER, Winter 2010, at 50-51, available at <http://www.medlawlegalteam.com/pdf/TrialReporterWinter-2010.pdf>.

Romano v. Steelcase

Kathleen Romano sued Steelcase, Inc. for personal injuries she allegedly sustained when she fell off her office chair while working at Stony Brook University.⁵³ Romano alleged that she suffered restricted movement of her neck and back and “pain and progressive deterioration with consequential loss of enjoyment of life”.⁵⁴ Steelcase sought to obtain copies of Romano’s Facebook and MySpace profiles for its defense.⁵⁵ It requested both the publicly available portions of her user profile as well as those portions that Romano had marked as private using the sites’ privacy settings.⁵⁶

To obtain the user profiles, Steelcase served Romano and the social networking sites with subpoenas.⁵⁷ Facebook objected to the request on the basis that releasing a user’s profile information without the user’s consent would be a violation of the SCA, which bars Facebook from “producing a non-consenting subscriber’s communications even when those communications are sought pursuant to a court order or subpoena”.⁵⁸ It also argued that Steelcase should request the communications directly from Romano rather than from Facebook.⁵⁹ MySpace did not take a position on the motion.⁶⁰ Romano refused to provide her consent and sought to quash the subpoena on privacy related grounds.⁶¹

In response, Steelcase argued that, based on the public portions of Romano’s Facebook and MySpace profiles, there was reasonable grounds to believe that Romano actually “has an active lifestyle and can travel and apparently engages in many other physical activities inconsistent with her claims in this litigation”.⁶² In support of this claim, Steelcase reported that Romano’s Facebook profile showed the plaintiff “smiling happily in a photograph outside the confines of her home despite the claim that she is largely confined to her house and bed”.⁶³

⁵³ Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (N.Y. Sup. Ct., Suffolk County 2010), *available at* http://decisions.courts.state.ny.us/fcas/fcas_docs/2010SEP/51000223320065SCIV.pdf.

⁵⁴ *Id.* at 653.

⁵⁵ *Id.*

⁵⁶ *Id.* at 654.

⁵⁷ Molly DiBianca, *Romano v. Steelcase: Defendant Granted Discovery of Plaintiff’s Facebook Profile*, DELAWARE EMPLOYMENT LAW BLOG (Sept. 27, 2010), http://www.delawareemploymentlawblog.com/2010/09/romano_v_steelcase_defendant_g.html.

⁵⁸ Marc J. Smith, *Court Orders Facebook to Produce “Private” Information*, MARYLAND EMPLOYMENT LAW BLOG (Sept. 27, 2010, 7:02 PM), <http://www.slgeemploymentlaw.com/blog/2010/9/27/court-orders-facebook-to-produce-private-information.html>.

⁵⁹ Noeleen G. Walder, *Judge Grants Discovery of Postings on Social Media*, LAW.COM (Sept. 24, 2010), <http://www.law.com/jsp/law/article.jsp?id=1202472483935>.

⁶⁰ Alexandra A Filutowski, *“Friends Only” Privacy Settings On Facebook Don’t Protect You From Insurance Companies*, FILUTOWSKI LAW FIRM BLOG (Sept. 27, 2010), <http://www.filutowskilaw.com/2010/09/friends-only-privacy-settings-on-facebook-dont-protect-you-from-insurance-companies>.

⁶¹ Vincent Cino, *Labor: “Private” Social Networking Activity Can Be Discoverable*, INSIDE COUNSEL (Oct. 25, 2010), <http://www.insidecounsel.com/Exclusives/2010/10/Pages/Private-Social-Networking-Activity-Can-Be-Discoverable.aspx>.

⁶² *Romano*, 907 N.Y.S.2d at 653.

⁶³ *Id.* at 654.

Romano countered that she “possesse[d] a reasonable expectation of privacy in her home computer”.⁶⁴ She argued that Steelcase’s claims of relevancy were based only on “speculation and conjecture” and characterized the discovery as a “blatant attempt by the defendant to intimidate and harass” her.⁶⁵ Romano further claimed that access to the private communications in Facebook and MySpace would give Steelcase access to “wholly irrelevant information as well as extremely private information”.⁶⁶

The New York Supreme Court that heard the case denied Romano’s motion to quash and ignored Facebook’s objection, ruling that precluding Steelcase from accessing Romano’s profiles “not only would go against the liberal discovery policies of New York favoring pretrial disclosure, but would condone [her] attempt to hide relevant information behind self-regulated privacy settings”.⁶⁷ It found that, based on the publicly available portions of Romano’s profiles, it was reasonable to conclude that the private portions “may contain further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action”.⁶⁸

The court also rejected Romano’s argument that the release of the information would violate her right to privacy. It reasoned that, by joining the social networking sites, Romano consented to the possibility that her personal information would be shared with others, notwithstanding her privacy settings.⁶⁹ The court stated, “[i]ndeed, that is the very nature and purpose of these social networking sites or they would cease to exist”.⁷⁰ It concluded that placing information on a site available to the public, or even to a few good friends, destroys privacy protection.⁷¹ The court ordered Romano to provide Facebook and MySpace with consent to disclose the information in the private portions of her social networking site profiles to the defendant.⁷²

Crispin v. Christian Audigier, Inc.

A court on the other end of the continent came to a very different conclusion. Buckley Crispin sued Christian Audigier for copyright infringement in a federal district court in California.⁷³ Crispin alleged that in late 2005 or early 2006, he granted Audigier and his company, Christian Audigier, Inc. (“CAI”), an oral license to use certain of his works of art in a limited manner in connection with the

⁶⁴ DiBianca, *supra* note 57.

⁶⁵ Gary Long, Greg Fowler & Simon Castley, *New York Trial Judge Orders Access to Private Facebook® and MySpace® Postings*, LEXOLOGY (Sept. 30, 2010), <http://www.lexology.com/library/detail.aspx?g=09503f39-1202-4775-85b0-703810bdf0d7>.

⁶⁶ Walder, *supra* note 59.

⁶⁷ *Romano*, 907 N.Y.S.2d at 655.

⁶⁸ *Id.* at 654.

⁶⁹ *Id.* at 657.

⁷⁰ *Id.*

⁷¹ Isom, *supra* note 9.

⁷² *Romano*, 907 N.Y.S.2d at 657.

⁷³ *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010), available at <http://www.minnesotaemploymentlawreport.com/Crispin%20v%20Christian%20Audigier.pdf>.

manufacture and sale of certain types of garments.⁷⁴ The agreement purportedly required that Audigier and CAI pay a specified sum for the right to reproduce each work of art on street-wear apparel.⁷⁵ It also required that they include Crispin's logo on each garment.⁷⁶

Crispin alleged that Audigier and CAI not only failed to include his logo on a substantial quantity of apparel bearing his artwork, but at times attributed the artwork to another artist or to Audigier himself.⁷⁷ Crispin also alleged that Audigier and CAI violated his rights further by sublicensing his artwork without obtaining his consent.⁷⁸ He contended that his artwork was being used on a variety of products that were outside the scope of the limited oral license he had granted the defendants.⁷⁹

Audigier served subpoenas duces tecum on Facebook, MySpace, and Media Temple (a web hosting service) seeking Crispin's subscriber information, all communications between Crispin and a witness, and all communications that referred to or were related to Audigier, CAI, or any sublicensees of his work.⁸⁰ Audigier contended that this information was relevant in determining the nature and terms of the agreement, if any, into which Crispin and Audigier entered.⁸¹

Crispin filed an ex parte motion to quash the subpoenas, arguing that the subpoenas sought communications that online service providers are prohibited from giving up under the SCA.⁸² Magistrate Judge John E. McDermott denied the motion, concluding that social networking sites were not electronic communications services that are protected under the SCA.⁸³ Citing *Quon v. Arch Wireless Operating Co.*, Judge McDermott held that in order to be considered ECS providers, social networking sites would have to "provide Internet access or operate as conduits for the transmission of data from one location to another" and that social networking sites did not meet this threshold because they were only used for public display.⁸⁴

District Judge Margaret Morrow agreed to hear Crispin's appeal of the magistrate judge's decision.⁸⁵ She ruled that the question of whether the communications were protected depended upon whether the social networking sites could be considered RCS providers or ECS providers under the SCA.⁸⁶ Judge

⁷⁴ *Id.* at 968.

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ *Id.* at 968-69.

⁸¹ *Id.* at 969.

⁸² *Id.*

⁸³ *Id.* at 969-70.

⁸⁴ *Id.* at 980. See *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008), available at http://scholar.google.com/scholar_case?case=1102310652013119778 (holding that SMS text messaging services qualify as "electronic communications services" under the SCA).

⁸⁵ Elaine Meyer, *Facebook, MySpace Messages Are Protected: Judge*, LAW360 (May 27, 2010), <http://contentclash.donigerlawfirm.com/oneclick/uploads/2010/05/facebook-myspace-messages-law360-ip-article.pdf>.

⁸⁶ *Crispin*, 717 F. Supp. 2d at 982.

Morrow found that Judge McDermott had misinterpreted the nature of social networking sites' messaging functions, not realizing that Facebook and MySpace have private messaging services which constitute an ECS.⁸⁷

In a lengthy decision, Judge Morrow reversed the ruling of Judge McDermott. The court held that private messages exchanged on Facebook and MySpace are no different than standard Internet e-mail exchanges that courts have already held are governed by the SCA.⁸⁸ Because the SCA prevents providers of communications services from divulging private communications and has no exceptions for service of legal process, the court quashed the subpoenas as they related to private messaging.⁸⁹ With respect to the Facebook wall postings and MySpace comments, the court remanded the matter to the magistrate judge to determine whether this information was publicly available.⁹⁰

This was the first time that a court analyzed whether private communications sent through a social networking site are afforded protection from disclosure under the SCA.⁹¹ The *Crispin* opinion illustrates that courts may afford social networking sites protection from disclosure of private electronic communications when such communications are requested via subpoena in a civil matter.⁹² However, as *Romano* demonstrates, requests for production directing a party to produce the private portions of a social networking site will generally be upheld over privacy objections.

Part II – Analysis

The SCA Provides No Real Privacy Protection in the Context of E-Discovery

When one analyzes the results of *Romano* and *Crispin*, it becomes clear that the SCA does little to protect any privacy rights that a litigant in a civil action might possess in his or her nonpublic social network site communications. Under *Crispin*, the opposing party cannot expect the social networking site to violate the SCA by producing the private communications of a subscriber. However, under *Romano*, the opposing party can avoid running afoul of the SCA simply by requesting the contents of a social networking site directly from the party via a Rule 34 request for production or, if necessary, asking the court to compel the user to provide his or her consent to disclosure of the information by the social networking service provider.

The illusory nature of the privacy protection provided by the SCA in the civil discovery context is illustrated by two cases. In *Barnes v. CUS Nashville*, the plaintiffs and several witnesses (all friends of the plaintiff) refused to comply with a Rule 34 request for production for the contents of their private

⁸⁷ *Id.* at 980.

⁸⁸ *Id.* at 979.

⁸⁹ *Id.* at 991.

⁹⁰ *Id.*

⁹¹ Scott A. Milner, *The Stored Communications Act: District Court Issues First Opinion on Privacy Protection for Information on Social Networking and Web Hosting Sites*, MORGAN LEWIS LAWFLASH (Jun. 14, 2010), http://www.morganlewis.com/pubs/eData_StoredCommAct_LF_14jun10.pdf.

⁹² *Id.*

Facebook communications, contending that they were private and irrelevant to the suit.⁹³ The defendant filed a motion to compel production.⁹⁴ In order to perform an in camera inspection of the content, District Judge Joseph B. Brown ordered the plaintiffs and witnesses to “friend” Magistrate Judge John T. Nixon on Facebook so that he could examine the content, thereby removing privacy protections as a barrier to disclosure.⁹⁵

In Flagg v. City of Detroit, which was filed by the minor son of a woman whose 2003 murder remained unsolved, the plaintiff alleged that Detroit officials deliberately concealed evidence obtained in their investigation, depriving the plaintiff of the opportunity to bring a wrongful death suit.⁹⁶ In early 2008, the plaintiff issued two subpoenas to Detroit’s third-party provider of text messaging services, SkyTel, seeking production of messages sent or received by various city employees.⁹⁷ The city moved to quash the subpoenas, arguing that the SCA prohibited the disclosure of its text messages by SkyTel.⁹⁸ The court ordered production of the text messages to go forward as planned, subject to in camera review, but only after the plaintiff reissued its demand in the form of Rule 34 requests for production directed to the city instead of subpoenas to Skytel.⁹⁹ In so doing, the court “avoid[ed the] question” of whether the text messages would also need to be produced pursuant to a third-party subpoena¹⁰⁰.

Social Networkers Have a Reasonable Expectation of Privacy

Users of social networking sites have a reasonable expectation of privacy for information stored in nonpublic areas. There are several reasons why this is so. First, especially for subscribers that utilize the privacy settings of social networking sites, these users have taken affirmative steps to maintain the confidentiality of communications made in non-public areas.¹⁰¹ Second, the privacy policies of social networking sites lead users to expect privacy, as these documents usually promise both security and confidentiality.¹⁰² Finally, social networking sites provide a very personalized experience and people

⁹³ *Barnes v. CUS Nashville, LLC*, No. 3:09-cv-00764, 2010 WL 2196591 (M.D. Tenn. Jun. 3, 2010), available at http://scholar.google.com/scholar_case?case=12902701719041969997.

⁹⁴ Nadine R. Weiskopf, *Social Media and E-Discovery: New Tools and New Challenges*, LEXIS NEXIS (2010), at 3, http://www.lexisnexis.com/Community/LitigationResourceCenter/cfs-filesystemfile.ashx/_key/CommunityServer.Components.SiteFiles/Documents.LRC Documents/White-Paper-Social-Media-and-E-2D00-Discovery--New-Tools-and-New-Challenges.pdf.

⁹⁵ Venkat Balasubramani, *Judge Offers to Facebook 'Friend' Witnesses in Order to Resolve Discovery Dispute – Barnes v. CUS Nashville*, TECHNOLOGY & MARKETING LAW BLOG (Jun. 9, 2010, 10:56 AM), http://blog.ericgoldman.org/archives/2010/06/judge_offers_to.htm.

⁹⁶ *Flagg v. Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008), available at <http://www.electronicdiscoveryblog.com/cases/flagg.pdf>.

⁹⁷ *Id.* at 348.

⁹⁸ *Id.*

⁹⁹ *Id.* at 367.

¹⁰⁰ *Id.* at 366.

¹⁰¹ Facebook and MySpace possess granular privacy settings that members can leverage to make confidential information nonpublic. William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105, 1114 (2009).

¹⁰² See, e.g., *Privacy Policy*, FACEBOOK, <http://www.facebook.com/policy.php> (last updated Oct. 5, 2010) (touting its eTrust certification); *Privacy Policy*, MYSPACE, <http://www.myspace.com/Help/Privacy> (last updated Feb. 20, 2008) (indicating its use of “commercially reasonable efforts” to protect user privacy).

utilize them the way that earlier generations utilized diaries and clubhouses. In fact, it often comes as a great surprise to users of social networking services that information communicated in nonpublic areas might be utilized in a legal proceeding.¹⁰³

“Private” Information in Social Networking Sites Should Remain Discoverable

The more critical question, however, is not whether social networking site users have a reasonable expectation of privacy, but whether this expectation should prevent discovery of non-privileged and relevant nonpublic information stored on social networking sites. For a number of reasons, this question should be answered in the negative.

First, as discussed in Part I, privacy is not the same as privilege. Privileges protect certain communications between litigants and specific individuals (e.g., attorneys, physicians, etc.). Each privilege serves a specific public policy purpose (e.g., to encourage frank discussions between attorneys and their clients). The creation of a “privacy” privilege encompassing all non-public communications with anyone would permit parties to shield relevant evidence from courts simply by storing it in a private portion of a social networking site. This would hamper the truth seeking process and foil a legal system based on the idea of liberal discovery.

Second, discovery does not necessarily result in public disclosure. Just because something is made available to another party or the court in a lawsuit through discovery does not mean that it will be disclosed to the public. The information can be subject to a protective order limiting disclosure or the record can be sealed.

Third, parties that engage in “litigant duplicity” should not be permitted to utilize privacy as a shield to legitimate fact finding. Allowing individuals to keep contradictory information out of litigation simply by placing it in the private portions of a social networking site will facilitate the commission of fraud on the court.

Finally, almost all other “private” communications, if relevant to the pending proceedings and non-privileged, are discoverable. Private e-mails are discoverable.¹⁰⁴ The contents of a diary are discoverable.¹⁰⁵ Confidential corporate memorandums are discoverable.¹⁰⁶ There is no reason to distinguish the private contents of a social networking site from any other private communication.

¹⁰³ Eric Goldman, *Deleted Facebook and MySpace Posts Are Discoverable – Romano v. Steelcase*, TECHNOLOGY & MARKETING LAW BLOG (Sept. 29, 2010), http://blog.ericgoldman.org/archives/2010/09/deleted_facebook.htm.

¹⁰⁴ *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 317 (S.D.N.Y. 2003), http://www.electronicdiscoveryblog.com/cases/zubulake_1.pdf.

¹⁰⁵ *Rexford v. Olczak*, 176 F.R.D. 90, 93 (W.D.N.Y. 1997).

¹⁰⁶ *Bird v. Penn Central Co.*, 61 F.R.D. 43 (E.D. Penn. 1973).

Part III – Proposal

The SCA Should Be Amended to Clarify Its Interaction with Discovery Rules

As demonstrated in Part II, because a party can obtain private content on social networking sites directly from the opposing party via a Rule 34 request for production and the court can compel compliance with the request, the SCA's prohibition against disclosure of subscriber communications by the social networking service provider is essentially superfluous. Since the SCA provides no meaningful privacy protection to civil litigants in discovery, its use in this context only serves to needlessly increase the complexity of litigation.¹⁰⁷ The SCA should therefore be amended to include an explicit exception for valid civil subpoenas modeled after the existing exception for court approved search warrants.¹⁰⁸

Advantages of the Proposal

There are several advantages of creating a civil subpoena exception to the SCA. Most importantly, it would eliminate the confusion that currently pervades the interaction between discovery and privacy in the context of social networking sites. With knowledge that the use of privacy settings in social networking sites will not provide subscribers with a "shield" against discovery in civil litigation, people would arrange their affairs accordingly (i.e., not post information they wish to remain "secret" on Facebook or MySpace).

Second, a civil subpoena exception would enhance the truth seeking process that serves as the primary purpose of broad and open discovery. By allowing a litigant to obtain relevant information directly from the social networking site instead of being forced to seek it from the opposing party, the possibility for spoliation and / or incomplete production due to the obvious bias of the producing party is eliminated.

Finally, a civil subpoena exception does no harm to the substantive privacy rights of the social networking site subscriber. As discussed in Part II, the privacy protection created by the SCA is largely illusory in the context of civil discovery, where a "privacy privilege" has never existed. Furthermore, protective orders would continue to be an option for anyone wishing to prevent the public disclosure of discoverable information. Thus, the elimination of the SCA as a bar to civil discovery would have little meaningful impact on privacy rights.

Expected Criticisms of the Proposal

One potential criticism of this proposal is that eliminates one of the few privacy protections currently available to social networking site users. However, given the elusive nature of the protection offered by the SCA in the context of civil discovery, its existence may actually do more harm than good. If meaningful privacy protections are proposed for social networking site users, they may be met with

¹⁰⁷ David D. Johnson, *How Private Posts on Social Media Can Lose Important Protections from Civil Discovery*, INTERNET AND E-COMMERCE LAW BLOG (Nov. 10, 2010), <http://www.internete-commerce.com/2010/11/articles/wiretap-laws/how-private-posts-on-social-media-can-lose-important-protections-from-civil-discovery>.

¹⁰⁸ The SCA's exception for a court approved search warrant can be found at 18 U.S.C. § 2703(b)(1)(A).

the retort, “since the SCA already offers privacy protection, there is no need for change”. Thus, the elimination of ineffective protection may be necessary to pave the way for meaningful reform.

Another potential criticism of this proposal is that it may shift the burden of producing discoverable information from the subscriber, who is a party to the litigation, to the social networking service provider, who is an innocent non-party. However, the social networking service provider is in a far better position to retrieve relevant information – both from a technical standpoint and without party bias. Additionally, as illustrated by *Romano*, a court can and will order the subscriber to provide consent to the social networking site for disclosure of his or her private communications.¹⁰⁹ In this case, the social networking service provider must endure the time and expense of producing the information anyway. Furthermore, the social networking service provider, not unlike banks and other frequently subpoenaed institutions, can charge a reasonable fee to recoup the costs of fulfilling such requests.

Conclusion

Social networking sites such as Facebook and MySpace have created a novel battleground for an age-old battle between open discovery and individual privacy. A number of recent cases applying age-old civil discovery rules and the CDA to disputes involving requests for non-public content on social networking sites have created an untenable situation where subscribers can shield content from disclosure by social networking sites but cannot stop their adversary or the court from compelling them to disclose the same information. Although social networking site users have a reasonable expectation of privacy in their non-public communications, that expectation should not be wielded as a shield to prevent proper civil discovery. Fortunately, this situation can be remedied by adding an exception to the SCA permitting the disclosure of non-public subscriber content pursuant to a valid civil subpoena. With this loophole closed, privacy advocates can focus on developing more meaningful privacy protections for social networkers.

Bradley J. Schaufenbuel is currently Senior Vice President and Information Security & Privacy Officer at Midwest Bank & Trust Company, now a part of FirstMerit Bank, N.A. He has held information security and privacy leadership positions at Zurich Financial Services, Experian Information Solutions, and Arthur Andersen LLP. Bradley is the author of “E-Discovery and the Federal Rules of Civil Procedure: A Pocket Guide”, published by IT Governance Publishing. He has also co-authored two “For Dummies” books and has had several articles published in professional journals on a wide variety of topics related to IT security and governance. Bradley holds 17 professional designations in the areas of information security management, IT compliance, fraud examination, IT audit, computer forensics, ethical hacking, information privacy, and project management. He possesses an MBA from DePaul University’s Kellstadt Graduate School of Business and is completing joint JD and LLM degrees in IT and privacy law at the John Marshall Law School in Chicago.

¹⁰⁹ Under the SCA, an online service provider is lawfully permitted to disclose the contents of an electronic communication to a third party with the subscriber’s expressed consent. 18 U.S.C. § 2702(b)(3).

National Security Officials Want Enhanced Capability to Intercept Communications Over the Internet

By Kathryn R. Coburn



Businesses that provide Internet Services can look for new government regulations in 2011. At a meeting of law enforcement officials in October 2010, FBI Director Robert Mueller warned the audience of the growing role of the Internet as a tool in spreading terrorism. In the words of Director Mueller, "The Internet has become a facilitator-even an accelerant- for terrorist and criminal activity." He emphasized the importance of technology in meeting that threat through the use of searchable databases that find connections and patterns in the information gathered through the intelligence community.

He voiced a concern that federal laws are not keeping pace with advancements in technology. According to Director Mueller, some companies that enable communications are not able to provide the electronic communications that the FBI seeks in response to a court order. Many communications providers are not currently required to build or maintain intercept capabilities in their operating systems and therefore, are not able to provide timely assistance to law enforcement.

The FBI is not alone in seeking enhanced intercept capabilities. President Obama has assembled a task force of government officials from the Justice Department, the National Security Agency and other agencies to address the problem.

On September 27, 2010, The New York Times reported that federal law enforcement and national security officials are preparing to seek sweeping new regulations for the Internet. According to the report, officials want Congress to require all services that enable communications- including encrypted e-mail transmitters like Blackberry, social networking Web sites like Facebook and software that allows direct "peer-to-peer" messaging like Skype, to be technically capable of permitting government agencies to intercept communications if the provider is served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages. The Times report said that officials from the FBI, the Justice Department, the National Security Agency and other agencies had been meeting with the White House to develop a proposal that the Obama administration plans to submit to Congress next year.

The proposal could have broad implications. The legislation is reported to include companies that operate from servers abroad, like Research in Motion, the Canadian maker of BlackBerry devices. Security services around the world face the similar problems and U.S. laws could be used as a model for other countries.

The likely elements of the legislation were reported by PC Magazine's Security Watch to be three:

- Communications services that encrypt messages must have a way to unscramble them.
- Foreign-based providers that do business inside the United States must install a domestic office capable of performing intercepts.
- Developers of software that enable peer-to-peer communication must redesign their service to allow interception.

Legislation to intercept communications is not new. Telephone networks in the U.S. are currently required to have intercept capabilities (backdoors) under a 1994 law called the Communications Assistance to Law Enforcement Act (CALEA).

CALEA was enacted in 1994 to mandate backdoors in U.S. telephone switches. CALEA currently requires telecommunications companies to install only telephone-switching equipment that meets detailed wiretapping standards. Federal regulators have expanded CALEA to cover Internet service providers and some voice-over-Internet companies, such as Vonage, and require them to retrofit their networks for government surveillance. Now the FBI logs directly into the telecom's network. After a court order has been sent to a carrier and the carrier turns on the wiretap, the communications data on the surveillance target streams into the FBI's computers in realtime. Communications networks like Skype, using peer-peer telephony, have posed intercept problems for the FBI's wiretapping engineers, due to lack of a central hub that can be tapped.

Law enforcement authorities now wish to expand CALEA to cover all providers that enable Internet communications.

On October 18, 2010, The New York Times published a second article on agency efforts to expand communications surveillance laws, *Officials Push to Bolster Law on Wiretapping*. The Times reported that An Obama administration task force that includes officials from the Justice and Commerce Departments, the FBI and other agencies recently began working on draft legislation to strengthen and expand CALEA, noting that there is not yet agreement on the details.

Balancing privacy and security is a huge challenge. As a result of revolutionary advances in technology and encryption, an increasing amount of business information is now being sent over electronic networks. Businesses have an interest, most often an obligation, to keep their proprietary information secure, private, confidential and out of unauthorized hands, such as competitors, criminals and foreign governments. In response to consumer demand for Internet security to ensure privacy, computer companies have continued to develop improved encryption software and hardware. Many of these encryption services are offered by communications providers. At this point, the government has not identified whether communications providers would be required to unscramble all encrypted messages sent over their networks, or only those using encryption offered by the provider.

James X. Dempsey, Vice President of the Center for Democracy and Technology, was quoted in the New York Times, saying the Obama proposal for new CALEA regulations is actually a request for

“authority to redesign services that take advantage of the unique and now pervasive, architecture of the Internet”. On the other hand, Valerie E. Caproni, General Counsel for the FBI, has been quoted as saying that “We’re not talking about expanding authority. We’re talking about preserving our ability to execute our existing authority in order to protect the public safety and national security.”

Not everyone agrees. The Electronic Frontier Foundation (“EFF”), an industry watchdog and civil liberties advocate, believes that making the Internet CALEA-compliant could actually backfire, claiming that many of the technologies currently used to create wiretap-friendly computer networks make the people on those networks more vulnerable to attackers by introducing more points of vulnerability in the system.

The EFF thinks that law enforcement may currently have, at its disposal, all of the surveillance capabilities and tools it needs to protect against terrorist activities and may not require new legislation under CALEA. The EFF recently sued the Justice Department for an injunction under the Freedom of Information Act, demanding FBI records concerning the Justice Department’s “Going Dark” Advanced Surveillance Program. The Foundation alleges that there is no public data about how often court-approved surveillance is frustrated because of a service’s technical design.

No one has identified who will be paying for compliance with the new regulations. There will be ongoing system maintenance and engineering changes as technology advances. Rewriting code can be pricey. Compliance will hit the smaller firms hardest and could cause financial problems if they are not reimbursed. On the other hand, if the government pays to cover the costs, the money will come from taxpayers. There is also the question of whether the federal government has the resources to create an effective system of oversight to assure that civil liberties of U.S. citizens are not infringed. Or whether reasonable oversight is even possible, given the inherent lack of transparency that such a system would entail and the government’s common practice of outsourcing portions of electronic security administration to private third parties.

These issues must be resolved as the legislation is being drafted and works its way through Congress.

Kathryn Coburn is a founder of Health IT Law Group in Los Angeles, California. Kathryn is health lawyer focused on healthcare information technology transactions, security and privacy issues and intellectual property. She assists clients in drafting and negotiating contracts for the acquisition, licensing, marketing, transfer and distribution of information technology. Kathryn is a managed care health lawyer in working in security, privacy and electronic transactions under HIPAA and the HITECH Act. She counsels clients on electronic data interchange, electronic health records and health information exchange operations. Prior to founding Health IT Law Group, Kathryn was Chief Technology Counsel to a nationwide Fortune 400 health plan, where she advised an all-payor healthcare clearinghouse and a Pharmacy Benefit Management Plan, creating strategic alliances and negotiating agreements for technology licensing, electronic data interchange, software acquisition and software development. Kathryn is Co-Chair of the Information Security Committee of the American Bar Association and Editor of the California Health Law News.

Knocking on the Cloud's Door - Obligations of Cloud Service Providers to Maintain the Privacy of Information Entrusted to Them

By Yakov Ginzburg



When asked whether users should be sharing information with Google as if it were a "trusted friend," Eric Schmidt, then-CEO of Google, Inc. (one of the major cloud service providers), responded, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."¹ Such cavalier attitude toward privacy from the head of a major cloud provider is very surprising. While criminals, terrorists, and social deviants may use the Cloud to achieve their illicit goals, the Cloud is mainly used for legitimate purposes. Law-abiding citizens use the Cloud to store

their data that may include highly personal information such as medical and financial data, digital calendars, photographs, diaries, and correspondence. Businesses and government entities use cloud to store commercially sensitive, proprietary and trade secret materials.²

In addition, despite of its young age, the Cloud has become a lucrative business with a bright future. Forrester Research estimates that various cloud services generated sales of more than \$12 billion in 2010.³ Having established itself solidly in productivity tools' and collaboration world (think Google Apps), the Cloud is poised to become a new delivery platform in new areas, such as data-intensive medical imaging.⁴

Although some people in high-tech industry believe that online "privacy is dead", general public, businesses, and the US government agencies consider safeguarding privacy of the electronic data as an important issue.⁵ While in the eyes of the public and the law, the burden for data security and privacy falls on the organizations that collect the information in the first place, the cloud providers may also be responsible for safeguarding the privacy of the entrusted data.⁶ Ensuring privacy of the cloud-stored information is a concern, which cloud providers simply cannot ignore.

Because of its unique distributed architecture, cloud computing creates complex jurisdictional issues when it comes to privacy. In the cloud environment, given the potential movement of data among

¹ Available at: <http://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy>

² J. Beckwith Burr, *The Electronic Communications Privacy Act of 1986: Principles for Reform*, at 4-5, available at: http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf

³ See generally, *Tanks in the cloud*, December 29, 2010, available at http://www.economist.com/node/17797794?story_id=17797794.

⁴ Vijay Vaitheeswaran, *A very Big HIT*, January 2011, *The World in 2011*, *The Economist* (Print Edition).

⁵ See generally, Epic.org, section on Cloud computing, available at <http://epic.org/privacy/cloudcomputing/>. See also Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies, at 3, August 2010, available at: <http://www.cio.gov>

⁶ Tim Mather et al., *Cloud Security & Privacy*, Kindle Edition, (2009), at 4,292.

multiple jurisdictions, the data housed in a jurisdiction is subject to the laws of that jurisdiction, even if its owner resides elsewhere. Thus, when evaluating their privacy obligations, US-based cloud providers must consider federal, state, and, possibly even foreign privacy regulations. Finally, the cloud providers should consider negotiating privacy provisions in their cloud service agreements.

U.S. Constitution, Federal Laws and Regulations

The U.S. privacy regulatory regime is a complex combination of the constitutionally-guaranteed privacy rights, sector-specific federal privacy laws, and state laws.⁷ At the federal constitutional level, both the First and Fourth Amendments offer some degree of informational privacy protection. However, constitutional privacy rights operate only against “state actors.” Private parties are protected but not bound by constitutional rights. Thus, unless Google satisfies the “state action doctrine,” one cannot maintain a 1st or 4th amendment claim against it.⁸

Still, government actors, such as intelligence and law enforcement officials, often seek access to private data maintained in the cloud (or on local hard drive for that matter). Thus the constitutional dimensions of privacy law can be highly relevant.

The Fourth Amendment to the United States Constitution

Currently a constitutional debate is ongoing in the United States over whether or not the Fourth Amendment covers information stored in the Cloud.⁹ The Warrant Clause of the Fourth Amendment fully protects the privacy rights of individuals in their information against the searches by the government if the data is stored on their computer’s hard-drive.¹⁰ However, the extent of the Fourth Amendment protections of privacy becomes less clear in cloud computing context where data has been entrusted to third-parties.

A judicially-developed “third-party doctrine” may allow the government to obtain personal information stored in the Cloud without a showing of probable cause.¹¹ Under the “third party doctrine”, if users voluntarily disclose their information to a third party, they can no longer have a reasonable expectation of privacy, and lose their Fourth Amendment rights in the revealed information.¹² As a result, cloud-stored information is repeatedly not considered to be falling under the “reasonable

⁷ See Mather, at 4,420 – 34.

⁸ However, federal statutes and state law may impose security and privacy obligations on private parties. There is no “state action” requirement here. See *infra* for further discussion of statutory rights.

⁹ See blog post *Privacy In The Clouds*, available at: <http://peacepalacelibrary-weekly.blogspot.com/2010/06/privacy-in-clouds.html>. See also generally, David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Expectations in Cloud Computing*, Minn. Law. Rev., 2009.

¹⁰ See Burr, at 6.

¹¹ Available at: http://blog.ericgoldman.org/archives/2010/01/4th_amendment_u_1.htm

¹² Kerr

expectation of privacy” doctrine as the information has been ‘handed’ over to third parties and is no longer considered to be private.¹³

Stored Communications Act

The Stored Communications Act (SCA)¹⁴, a component of the broader Electronic Communications Privacy Act (ECPA),¹⁵ generally prohibits electronic service providers from disclosing their customers’ information without a warrant and a prior notice to the customers. However, the SCA can give users a false sense of security with respect to their privacy.”¹⁶ While cloud users may assume that the SCA fully protects their privacy in their emails or electronic documents, determining whether and how their privacy is actually protected requires a complex analysis.

First, the SCA only regulates providers that fit within two categories defined by the Act. If the SCA regulates an entity, it protects its customers’ communication. Otherwise, only the Fourth Amendment protections, diminished by “third-party doctrine,” apply. Second, the SCA only protects “content of electronic communications,” leaving non-content data outside of its orbit of influence. Finally, under certain circumstances, the SCA allows the electronic providers to disclose their customers’ data without a warrant or prior notice. We will explore how cloud providers, such as the Google Apps, fare under the SCA.

The SCA recognizes two types of the service providers: Electronic Communication Service (ECS) and Remote Communication Service (RCS).¹⁷ To qualify as ECS, entities must provide users with the ability to send or receive electronic communications,” and hold the electronic communication in “electronic storage.” The SCA limits “electronic storage” to “temporary, intermediate storage ... incidental to the electronic transmission” of the communication and copies made by the service provider for “backup protection.”¹⁸

Google Apps satisfies first requirement by offering an email application (Gmail) that allows users to send and receive electronic emails. However, the Apps do not hold the electronic communications in the electronic storage within the meaning of the SCA because they allow users to indefinitely store various electronic documents both created by the Apps and uploaded from the users’ hard-drives. Additionally, the Apps offer its customers the ability to store 5000 documents and presentations, in addition to 1000 spreadsheets - far more than any customer may need for temporary purposes.¹⁹ Thus, the Apps will not be considered an ECS.

¹³ See sources cited in note 24, *supra*.

¹⁴ See 18 U.S.C. §§ 2701 - 2712

¹⁵ See 18 U.S.C. §§ 2510 - 2522

¹⁶ See Mather at 4,486 – 96.

¹⁷ See 18 U.S.C. §§ 2510, 2711 respectively.

¹⁸ William J. Robinson, *Free At What Cost?: Cloud Computing Privacy Under The Stored Communication Act.*, Georgetown Law Journal, April 2010, at 1206.

¹⁹ See *Id.* at 1210.

To qualify as RCS, service providers must satisfy four requirements. First, the provider must offer “computer storage or processing services” to the public through an electronic communications system. Second, the data must be received electronically from the customer. Third, the content must be “carried or maintained” by the service provider “solely for the purpose of providing storage or computer processing services” to the customer. Finally, the provider cannot be “authorized to access the [customer's] content for purposes of providing any services other than storage or computer processing.”²⁰

The Apps easily satisfy the first three requirements. However, the Apps will not satisfy the fourth requirement if customers authorize access to their data for the provision of contextual or targeted advertising services. For example, to support its “free model,” Google allows “targeted ads” to display in the users’ email messages.²¹ In order to provide relevant advertisement messages to its customers, Google automatically scans all the email messages to match words in the emails to advertisements that offer relevant products.²² Since all Gmail customers must agree to this feature in exchange for a free email account, the Apps status as a RCS is compromised.²³

Even if cloud providers pass the muster of “archaic distinctions”²⁴ imposed by the SCA, not every type of data stored on the providers’ computers is protected. The so-called non-content or transactional data, which may include personal identifying information about the user, such as her name, physical or e-mail addresses, and IP address, is entitled to little protection. A service provider can voluntarily disclose the user's personal identifying information to any non-governmental entity or provide it directly to the government upon receipt of an administrative subpoena.²⁵

In addition, it is unclear whether the SCA protects privacy of all kinds of the “content” data. The SCA clearly protects email messages.²⁶ Other types of content created using cloud services such as word documents, spreadsheets, presentations or video may be protected under the SCA.²⁷ On the other hand, at least one court held that text messages stored in the Cloud are not protected by the SCA.²⁸

Even if the SCA protects electronic data from disclosure, the government can still obtain the information without a warrant under two specific circumstances. First, data stored in an RCS for any duration may be accessed by the government through a section 2703(d) order requiring only

²⁰ See *Id.* at 1213.

²¹ Companies like Google and Facebook make money by targeting ads to people based on their Internet browsing behavior. It is a critical aspect of their business model. See generally an article available at: http://money.cnn.com/2010/12/02/technology/ftc_do_not_track/index.htm

²² See Gmail privacy policy at: http://mail.google.com/mail/help/about_privacy.html#scanning_email

²³ See Robinson, for examples of other cloud providers scanning users’ content, at 1217.

²⁴ Mike Masnick, *Does Storing Your Documents In “The Cloud” Mean The Gov’t Has Easier Access To It?*, May 5, 2010, available at : <http://www.techdirt.com/blog.php?d=5&m=5&y=2010>

²⁵ See Robinson at 1208.

²⁶ See 18 U.S.C §2703(b) for some important limitations. See also discussion of §2703(b) exception, *infra*.

²⁷ See discussion of *Viacom* case, Robinson at 1219.

²⁸ See discussion of *Flagg* case, Robinson at 1218.

“reasonable grounds to believe” the data is “relevant and material to an ongoing criminal investigation.”²⁹ Second, the SCA allows the government to compel certain types of electronic communications with administrative subpoenas. For e-mail communications in electronic storage for 181 days or more, the SCA allows the government to compel disclosure of these private e-mail communications by an administrative or grand jury subpoena, or court order if the government “offers specific and articulable facts showing that... the contents of a wire or electronic communication are relevant and material to an ongoing investigation.” Under both exceptions, the government may delay notification of the party whose information was compelled up to 90 days. Effectively, this exception negates notice requirement.³⁰

Although the government has been routinely required to obtain search warrants or use subpoenas to compel email communications, procedure for compelling other types of documents created and stored in the Cloud is not clear. In one case, the FBI was able to retrieve documents stored on the Google Docs "cloud" word-processing service, in an investigation of a company accused of sending spam emails to millions of people.³¹ However, at least in one case the “court appears to have diminished some of these protections by allowing governmental entities to obtain cloud-based e-mails (and other electronic communications) directly from the service provider with only a trial subpoena and not a warrant as previously required.”³²

USA PATRIOT Act

The PATRIOT Act allows law enforcement agencies to compel “virtually any document, including electronic documents held by cloud providers.”³³

Section 215 of the PATRIOT Act amended the business record sections of FISA³⁴ to authorize the Director of the FBI to apply to the FISA court for orders granting the government access to any tangible item (including books, records, papers, and other documents), no matter who holds it, in foreign intelligence, international terrorism, and clandestine intelligence cases.³⁵

²⁹ Martin C. Weinberg & Robert M. Goldstein, *The Stored Communications Act and Private E-Mail Communications*, available at:

<http://www.nacdl.org/public.nsf/698c98dd101a846085256eb400500c01/34c7516bee49134a852573620050727d?OpenDocument>

³⁰ *Id.*

³¹ See blog post, *Search Warrants in the Sky: FBI Collects Info from Google Docs*, available at:

<http://citmedialaw.org/blog/2010/search-warrants-sky-fbi-collects-info-from-google-docs>

³² See generally Nolan M. Goldberg and Martha Willson-Byrne, *Securing Communications on The Cloud*, available at:

<http://www.infolawgroup.com/uploads/file/Goldberg%20Article.pdf>

³³ See Robert McHale, *Cloud Security and Privacy: A Legal Compliance and Risk Management Guide, Part 1*, May 3, 2010, available at: <http://www.informit.com/articles/article.aspx?p=1582936>

³⁴ Foreign Intelligence Surveillance Act (FISA), see generally FISA overview, available at:

<http://epic.org/privacy/terrorism/fisa/>

³⁵ See Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, World Privacy Forum, 2009 p.14, available at: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

The PATRIOT Act also allows the government to gain access to personal financial information and student information stored in electronic systems without providing notice to the owners of the data. The only requirement is governmental certification that the information obtained would be relevant to an ongoing criminal investigation. A cloud provider may be required to provide information on a cloud user or a cloud user's customers to the U.S. government without providing notice to the cloud user.³⁶ Additionally, Section 505 of the PATRIOT Act provides FBI with the ability to obtain personal customer records (such as e-mails, financial records, and consumer reports) from financial institutions and wire or electronic service providers using National Security Letters³⁷ without any prior court approval.³⁸

A possibility of facing a "215 Order" may affect a cloud provider's decisions about users' data location. For example, Google stores Google Apps' data in Canada-based data centers that are not subject to the PATRIOT Act.³⁹ Other large companies have routed their Internet traffic away from U.S. jurisdictions and started storing their data outside the U.S.⁴⁰

Gramm-Leach-Bliley Act

The two main provisions of the Gramm-Leach Bliley Act (GLBA), the Financial Privacy Rule⁴¹ and the Safeguards Rule, have a significant impact on privacy considerations for financial institutions storing data in the cloud.⁴² Various United States government agencies (such as the Federal Trade Commission – FTC) have implemented, and currently enforce the standards set by the GLBA.⁴³

The GLBA only regulates companies that are "significantly engaged" in the financial activities.⁴⁴ The financial institutions falling under the GLBA regulations include not only banks, securities firms, and insurance companies, but also companies that provide other types of financial services, such as non-bank mortgage lenders, loan brokers, some financial or investment advisers, credit counselors, tax preparers, providers of real estate settlement services, and debt collectors.⁴⁵

The Financial Privacy Rule regulates the collection and disclosure of customers' personal information by financial institutions and service providers. Under the GLBA, a service provider is "any number of

³⁶ *Id.*

³⁷ See definition of National Security Letter, available at: <http://epic.org/privacy/nsl/>

³⁸ See McHale.

³⁹ See blog post, Patriot Act May Jeopardize Cloud E-Mail Adoption, available at: http://blogs.channelinsider.com/cloud_computing/content/email_communications/patriot_act_may jeopardize_cloud_email_adoption.html

⁴⁰ Jeffrey F. Rayport, Andrew Heyward, *Envisioning the Cloud: The Next Computing Paradigm*, Marketplace LLC ii (2009) at 37, available at: <http://www.marketpaceadvisory.com/cloud/>. But see also McHale - Section 215 of the Patriot Act is set to expire on February 28, 2011.

⁴¹ See GLBA, Subtitle A, Disclosure of Nonpublic Personal Information, codified at 15 U.S.C. §§ 6801–6809

⁴² See generally http://itlaw.wikia.com/wiki/Safeguards_Rule#FTC_Safeguards_Rule

⁴³ *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*, at Federal Trade Commission, Bureau of Consumer Protection Business Center available at <http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act>

⁴⁴ *Id.*

⁴⁵ See McHale.

individuals or companies that provide services to the financial institution,” including cloud providers handling the personal information of a financial institution's customers. Hence, if a financial institution stores its customers' files in the Google Apps, Google will be considered a service provider under the GLBA.

The protections of the Financial Privacy Rule requires that financial institutions enter into a contract with a service provider prohibiting that service provider from disclosing or using the information in any manner other than to carry out the purposes for which the information was disclosed to it in the first place. Some cloud services may not be able to comply with this requirement. Suppose a financial institution uses a Gmail account to send emails containing customers' financial reports (e.g. account statuses, etc). In turn, Google automatically scans such email messages⁴⁶. As a result, Google may find itself violating the conditions of the Financial Privacy Rule.

The Financial Privacy Rule also requires financial institutions to provide their customers with privacy notices at the beginning of their services and annually thereafter, for the duration of their relationship with their customers. First, the notice must explain how the personal financial information is collected, shared, used and protected. Second, the notice must state that the customers have the right to opt out of having their personal financial information shared with “unaffiliated” third parties.⁴⁷

However, a problem arises when a service provider is an “affiliated 3rd party” and the opt-out provision is not available to customers. Under the GLBA, a service provider is an “affiliated party” if it meets the following three requirements: (1) the financial institution shares information with outside companies that provide essential services, like data processing or servicing accounts; (2) the disclosure is legally required; and (3) the financial institution shares customer data with outside service providers that market the financial company's products or services.⁴⁸

The distinction between “affiliated” and “nonaffiliated” entity for opt-out purposes can seriously affect viability of using cloud services by financial institutions. If cloud providers are deemed as “unaffiliated entities,” then the customers of the financial institutions can prohibit these institutions from sharing their private financial data. The prohibition will effectively prevent financial institutions from using the cloud services. It is still unclear, though, whether cloud providers are considered “unaffiliated” or “affiliated” under the GLBA.⁴⁹

While the “opt-out” option may provide privacy protections for nonpublic personal financial information for consumers, not doing so leaves service providers open to re-disclosure of customers' information received from financial institutions. If a customer does not opt out, the recipient of the information (e.g. the cloud provider) steps into the shoes of the disclosing financial institution, and

⁴⁶ See Robinson, for examples of other cloud providers scanning users' content, at 1217.

⁴⁷ See McHale.

⁴⁸ See sources cited in note 42, *supra*.

⁴⁹ See McHale.

may use the information for its own purposes, or re-disclose it to yet another third party, consistent with the financial institution's privacy notice.”⁵⁰ For instance, if a financial institution uses Google Apps to store its customers’ information, and the customers do not opt out, Google may be able use the institution’s customers’ information in exactly the same way as the institution could. This may be contrary to the customers’ expectation of privacy in their financial data.

The Safeguards Rule mandates that all financial institutions develop and maintain an information security program to protect nonpublic customer information.⁵¹ The Rule further requires financial institutions to monitor and test their security program. When a financial institution uses a cloud service to store its customers’ non-public financial data, the cloud service effectively becomes part of the financial institution’s security program. In such an arrangement, monitoring and testing of the security program may be challenging. Given the complexity of the safeguard requirements and potential size of a cloud provider’s user base, the provider may not be able to work with financial institutions individually to test their particular information security programs.⁵²

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA)⁵³ consists of two rules: the Privacy Rule (which limits disclosure of personal health information) and the Security Rule (which controls access to protected health information (EPI)).

Entities covered by these regulations include anyone transmitting health information in electronic form in connection with transactions covered by HIPAA. Personal information falling under the HIPAA protections is interpreted broadly enough to include anything from health status to payment for health services.⁵⁴

Any outsourcing of functions by the covered entity to business associates automatically makes the business associates fall under HIPAA regulations, and requires a signing of a “business associate contract” that binds the service provider to the same HIPAA privacy requirements that govern the covered entity. For example, if a doctor uses the Google Apps to store her patients’ information, Google will be considered the doctor’s “business associate.”

The business associate contract must specify the procedure by which the cloud service provider responds to subpoenas for patients’ records stored on behalf of a covered entity. HIPAA requires covered entities to notify the patient about any subpoena requiring the patient’s PHI and give the

⁵⁰ See sources cited in note 42, *supra*.

⁵¹ See Mather, at 4,533 - 44

⁵² See McHale

⁵³ Full Text of the HIPAA is available at: Pub. L. No. 104-191, 110 Stat. 1936 (Aug. 21, 1996).

⁵⁴ See generally http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

patient an opportunity to object. As a business associate, a cloud provider will also be bound by the same reporting requirement.⁵⁵

HITECH Act

The HITECH Act⁵⁶ significantly expands the HIPAA Privacy Rule and security standards, expands the rules for business associates, and adds provisions for breach notifications. The HITECH Act has expanded the number of entities covered by HIPAA and established increased accountability and liability to business associates.⁵⁷ The Act requires notification of a breach of unencrypted health records' breach notification (similar to that under state data breach notification laws) for all covered entities that are required to comply with HIPAA regulations.⁵⁸

The HITECH Act's expansive definition of covered entities may affect obligations of the cloud providers offering electronic health records (EHR) services. Unfortunately, the HITECH Act does not provide clear guidance on how to classify such EHR providers.⁵⁹ For example, Google Health is one of the cloud-based EHR providers that allow users to manage and share their health information.⁶⁰ Although Google Health claims that it does not have to comply with the HIPAA requirements because it is neither a covered entity nor business associate,⁶¹ the HITECH Act's expanded definition of a "business associate" may force Google Health under the auspices of HIPAA. Effectively, the HITECH Act turns such third-party data repositories, personal health records, and health information networks into business associates of the covered entities.⁶²

States Laws and Regulations

Some states have also enacted privacy laws and created agencies dedicated to enforcing these laws. Many states have statutes and regulations that are similar to the requirements of GLBA and HIPAA. Several states also have laws regarding the proper disposal of consumer information, use of social security numbers, and other similar protections. Under the state laws that regulate unfair and deceptive business practices, the states' Attorneys General can enforce laws for privacy violations.⁶³ Since cloud providers' operations may span multiple states and the customers' data may travel from state to state during its lifetime, the cloud provider will need to comply with the individual states' privacy laws.

⁵⁵ See McHale.

⁵⁶ Health Information Technology for Economic and Clinical Health Act (HITECH), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat 115, Feb. 17, 2009, 42 USC sec. 17931 et. seq.

⁵⁷ See Mather, at 4,566 - 77

⁵⁸ See Janine Anthony Bowen, McKenna Long & Aldridge LLP, *Cloud Computing 2010: Is Your Company Ready?* Practising Law Institute Intellectual Property Handbook Series, PLI Order No. 24066, June 2010, at 48.

⁵⁹ See Mather, at 4,588 - 99

⁶⁰ See How Google Health works at <http://www.google.com/intl/en-US/health/about/>

⁶¹ See Google notice about HIPAA compliance at: <http://www.google.com/intl/en-US/health/hipaa.html>

⁶² See Mather, at 4,588 - 99

⁶³ See Rebecca S. Eisner & Mark A. Oram, Mayer Brown LLP, *Clear Skies or Stormy Weather For Cloud Computing?*, PLI Course Handbook Series, PLI Order No. 25879 September-November 2010, at 431.

International Data Privacy Regime

European Union Data Privacy Directive

Unlike the United States, the European Union (EU) has a comprehensive privacy framework, the EU Data Protection Directive (Directive), governing written, oral, electronic, and internet-based data residing in the EU. Each member state has its own unique law implementing the Directive. The Directive distinguishes between data controllers and data processors. Data controllers and data processors have different roles and different sets of obligations related to privacy.

If an entity (person or an organization) has authority to make decision about the processing of data or determines the purposes and means of processing of the personal data, it is considered a data controller.⁶⁴ Article 17 of the Directive requires a data controller to “implement appropriate technical and organizational controls to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access...”⁶⁵

If an entity does not have decision making power with respect to the data processing and acts only on the instructions of the data controller or owner, it will be classified as data processor. Article 17 also mandates that there be a written contract between a data controller and a data processor, requiring that the data processor act only on instructions from the data controller.⁶⁶

Users of cloud service providers are usually classified as data controllers, because they retain decision making power on data processing issues. Alternatively, cloud providers are usually classified as data processors, because they process the customers’ data based on the customers’ instructions.⁶⁷ It is unclear whether the status of a cloud provider changes if it unilaterally decides to move its customers’ data from one of its servers to another. If this decision is considered a “decision about processing data,” then the cloud provider will be considered a “data controller.”

A key feature of the Directive is its extraterritorial effect. The EU prohibits the transfer of personal information of EU residents out of the EU to a vast majority of countries around the world (including the US) that do not meet the adequate level of data protection, as measured by the EU standards. A country has several ways of attaining “adequate levels of data protection.” The first way is to be one of the countries that have implemented laws that the EU deems to be “adequate protection.” Currently, those countries are Argentina, Canada, Guernsey, Isle of Man, and Switzerland. For the rest of the world adequate protection can be achieved through: (1) compliance with safe harbor provisions, (2) use of model contractual clauses prepared by the EU (for which strict conformance to the form

⁶⁴ See Mather at 4,615 - 27

⁶⁵ See Bowen, at 50.

⁶⁶ See *Id*, at 50.

⁶⁷ See Mather, at 4,628 – 38.

language is required), or (3) use of binding corporate rules.⁶⁸

In order to comply with the EU Directive, the U.S. Department of Commerce developed a “Safe Harbor Program” designed to protect accidental information disclosure or loss. U.S. Companies can opt into the program and self-certify that they have “adequate” privacy protections. “Adequate privacy protections” must satisfy seven Safe Harbor Principles: (1) notice; (2) choice; (3) onward transfer; (4) access security; (5) data integrity; and (6) enforcement. Once a company certifies that it has “adequate protections,” failure to follow its commitment may be actionable under federal and state laws prohibiting unfair and deceptive acts.⁶⁹

Under Article 4 of the Directive, EU’s jurisdiction over the data does not end even after the data has left EU territory. Once an EU member state’s data protection law attaches to personal information, there is no clear way to remove the applicability of the law to the data.⁷⁰ As a result, adoption of the cloud computing in Europe can be significantly inhibited.⁷¹

The Rest of the World

Many countries have data protection or data privacy regimes in place, but the coverage and effect of such regimes vary. As of November 2010, there are almost eighty countries with comprehensive privacy laws in effect, many of which have their own unique regulatory requirements. For example, Mexico, Malaysia, and Taiwan have adopted comprehensive national privacy laws that regulate the collection, use, and disclosure of personal information.⁷² Argentina’s and Canada’s regimes are similar to the EU approach.⁷³

India, a popular destination for outsourcing, recognizes a right to privacy against entities in the public sector, but has enacted only a limited number of privacy statutes with little coverage for the private sector.⁷⁴ Brazil, like many countries, has a constitutional right to privacy. However, Brazil has no comprehensive data privacy law. Instead it relies on a patchwork of sectoral laws. China’s constitution refers to privacy indirectly, but the country has very few specific laws.⁷⁵

Contractual Arrangements

While individual users of cloud computing services may rely on the privacy protections available under relevant federal, state and international laws and published Terms of Service, businesses and government entities can turn to contractual arrangements to strengthen privacy protections of the

⁶⁸ See Bowen, at 54.

⁶⁹ See McHale.

⁷⁰ See *Id.*, at 54.

⁷¹ Kevin J. O’Brien, Cloud Computing Hits Snag in Europe, N.Y. Times, September 19, 2010, *available at*: http://www.nytimes.com/2010/09/20/technology/20cloud.html?_r=2&ref=technology

⁷² See generally Cynthia Rich et. Al., International Data Protection Laws, Morrison & Foerster Client Alert, November 15, 2010, *available at*: <http://www.mofo.com/files/Uploads/Images/101115-International-Data-Protection-Laws.pdf>

⁷³ See Bowen, at 51.

⁷⁴ *Id.*

⁷⁵ See Bowen, at 51.

users' privacy. An organization's contractual agreement with a cloud service provider is perhaps the most critical component in evaluating cloud computing risks, including privacy.⁷⁶

Companies negotiating Cloud Service Agreements (CSA) should consider a list provisions to ensure privacy of their customers' data. First, CSA should clearly identify ownership of the data. Since the user's data will reside on a cloud computing company's infrastructure, it is important that the contract clearly affirms the user's ownership of the data.⁷⁷

Second, CSA should stipulate obligations of cloud providers to comply with applicable privacy laws. This is necessary because the data owner could be held liable if a service provider violates a privacy law applicable to the data owner.⁷⁸ Take, for example, Google's contract with City of Los Angeles to replace the city's existing e-mail system with Google Apps.⁷⁹ The Google Contract does not spell out Google's obligation with regards to privacy laws, despite the fact that it will be storing, processing and transmitting City of Los Angeles' information.⁸⁰

Third, SCA must prohibit cloud providers from unilaterally changing their privacy policy and terms of use. Ability to control the provider's changes in privacy policies ensures that the data owner does not lose control over the data stored with the provider.⁸¹

Fourth, the agreement should specify responsibilities of the cloud computing service provider as to legal or government requests for access to data by clearly stating how the service provider must respond to legal requests for information, and what notice opportunity for objection the cloud user is granted.⁸²

Fifth, the agreement must cover the cloud service provider's obligations in the event that the user's data is accessed inappropriately.⁸³ Enforcing the cloud provider's accountability for prompt breach notifications will ensure users' compliance with various state laws that primarily deal with data breach notifications.⁸⁴ Finally, to reduce cross-border jurisdictional issues related to privacy, users should limit

⁷⁶ See Robert McHale, *Cloud Security and Privacy: A Legal Compliance and Risk Management Guide, Part 2*, May 10, 2010, available at: <http://www.informit.com/articles/article.aspx?p=1586456>

⁷⁷ Thomas J. Trappier, *If It's in the Cloud, Get It on Paper: Cloud Computing Contract Issues*, EDUCAUSE Quarterly Magazine, Volume 33, Number 2, 2010, available at: <http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/IfitsintheCloudGetItonPaperClo/206532>

⁷⁸ David Navetta, *What's in Google's SaaS Contract with the City of Los Angeles? Part Two*, June 3, 2010, available at: <http://www.infolawgroup.com/2010/06/articles/cloud-computing-1/whats-in-googles-saas-contract-with-the-city-of-los-angeles-part-two/>

⁷⁹ See an announcement and details of the contract available at: <http://www.informationweek.com/news/services/saas/showArticle.jhtml?articleID=221100129>

⁸⁰ *Id.*

⁸¹ See generally sources cited in note 76, supra.

⁸² *Id.*

⁸³ See generally sources cited in note 77, supra.

⁸⁴ See Bowen, at 45.

the geographical location of their data.⁸⁵

Conclusion

In general, cloud service providers are responsible for ensuring privacy of the data entrusted to them. However, the extent of their responsibility may vary depending on a geographical location of the data and the provider, type of a provider, type of data, and the cloud service provider's contractual obligations.

Geographical location of the data determines the controlling jurisdiction that the cloud provider is subject to. For instance, if a cloud provider's processing facilities are located in California, both relevant California State and U.S. federal laws will govern the privacy of the customers' data. If the cloud provider transfers customers' data to its facilities in Europe, then EU laws will apply. Trans-border issues are exacerbated because the legal and regulatory regimes for data privacy vary from strictly enforced to non-existent.⁸⁶

In the U.S., the type of the cloud provider and the type of the data may define the privacy responsibilities of the cloud providers. To receive privacy protections under the SCA, users' data must be handled by a service provider that satisfies narrow definition of the regulated entity.⁸⁷ Privacy of financial data and health-related information is regulated by the GLBA and the HIPAA respectively. Finally, contractual terms can help users' companies strengthen the cloud providers' responsibility to safeguard privacy of the data.⁸⁸

Mr. Ginzburg works full-time as a software developer at The Capital Group Companies, Inc. Mr. Ginzburg has more than ten years of experience in developing web-based business applications in various industries including Telecommunications, Entertainment, Local Government, and Financials. Before joining The Capital Group Companies, Mr. Ginzburg worked as a staff IT consultant at Big 4 consulting companies Capgemini, LLC and BearingPoint, Inc. Mr. Ginzburg is a Patent Agent, and is a Certified Information Systems Auditor (CISA). Karl M. Manheim, Professor of Law, Loyola Law School, Los Angeles, provided useful feedback and inputs for this article. He is the Loyola director of the Program for Law & Technology at the California Institute of Technology and Loyola Law School.

⁸⁵ See generally sources cited in notes 76 and 77, supra.

⁸⁶ See Mather, at 4,401 – 11.

⁸⁷ See generally Robinson.

⁸⁸ See Mather, at 4,486 – 96.

Committee Co-Chairs' Message

Dear ISC Members:

Well, we did it. Our committee's book, titled *Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*, is being published the week of February 14, to coincide with the RSA conference in San Francisco. This essentially new book targets the three audiences described in its title which includes non-lawyers and those outside the U.S. Over sixty people were involved in the content creation, a true team effort writ large. Now comes the fun part, telling everyone about it. So we are asking the speakers at RSA to plug the book but beyond that, we would ask committee members, authors and non-authors alike, to make your peers, clients and professional networks aware of the book. See the first article in this issue for more information on this book.

This coming weekend, February 12-13, the committee will be having a pre-RSA meeting in San Francisco. This meeting, for which we will also try to provide remote and time-delayed access, will be held in the law firm offices of Foley & Lardner LLP. The topics covered include:

- Responding to a FTC Data Security Enforcement Action
- "Security Research and the Law"
- The Rise of "Hacktivism" Why COICA has Already Failed
- "Legally Defensible Security: the In-house Perspective"
- "Disclosure Requirements for Vulnerabilities and Security Breaches in Health Care"
- "Robotics Liability"
- "Bridging the Gap: How to Reduce Security Risk, Increase Resilience and Stop Wasting Money"
- "Legal Risks Associated with Business Partner Security Questionnaires"

Our committee also hosted a live webinar and teleconference on January 25 titled "Hot Topics in Information Security Law." The panel provided the most recent information on topics including the status of data security legislation, at the federal, state and international levels. They looked at regulators and enforcement and litigation involving the various data breaches, such as payment card data security breaches, consumer data breaches and online banking security breaches. The panel also covered cloud computing and social networking and their impacts on information security and privacy. Keep an eye posted for upcoming webinar announcements.

And we would like to welcome members of the SciTech section's E-Privacy Law committee who may be getting their first chance to read our periodical. Our editor reached out to the E-Privacy Law committee chairs for permission to extend the call for articles to their members as well and we were rewarded as one of the authors in this issue responded to that call with an article. Thank you to John Tomaszewski and the leadership of that committee for consenting to the wider circulation.

Also we continue to ask that you share your knowledge and experience with your fellow professionals and committee members by writing an article for this periodical. Our next issue (Summer 2011) will come out in June. That is it for now. We look forward to seeing you shortly in San Francisco for RSA.

David Navetta,
ISC Co-Chair