Report of the
New York State Bar Association's
Task Force on Privacy

For the Consideration of the House of Delegates ■ April 4, 2009

Acknowledgements

The Members of the Privacy Task Force respectfully submit this updated Report for approval by the House of Delegates at its regularly scheduled meeting to be held on April 4, 2009 in Albany, New York.

The Task Force members would like to specially acknowledge the following individuals, whose help and assistance made this Report possible.

- Matthew Barach, Internet & Information Privacy Counsel, New York State Consumer Protection Board, Albany, New York
- Christopher Calabrese, American Civil Liberties Union
- Deepica Capoor, Associate, Powley & Gibson, P.C., New York, New York
- Robert Ellis Smith, Publisher, Privacy Journal Newsletter
- Prashant K. Jha, BA, LL.B., LL.M., New Delhi, India
- Kevin Kelly, Prisoner's Legal Services, Ithaca, New York
- Jason Mazzone, Professor, Brooklyn Law School, Brooklyn, New York
- Jason Oliver, Associate, Baker Hostetler, Fellow, NYSBA Intellectual Property Law Section, New York, New York
- Brynn Rovito, Student, Brooklyn Law School and Legal Intern, The American Society for the Prevention of Cruelty to Animals, New York, New York
- Dana Schuessler, Martha Stewart Omnimedia, New York, New York
- Alexander van Gaalen, Registered Patent Agent; Student, Benjamin N. Cardozo School of Law; Fellow, NYSBA Intellectual Property Law Section, New York, New York
- Stacey Whiteley, Liaison, NYSBA Privacy Initiative, Program Manager, Law, Youth and Citizenship Program, NYSBA, Albany, New York
- Richard Weitzman, Bronx County Bar Association, New York, New York

The Task Force would also like to thank the following members of the New York State Bar Association who participated in and provided invaluable insight at the Privacy Summit on March 5, 2009:

- Kenneth Bond, Municipal Law Section
- Tammy Lawlor, Elder Law Section

- Matthew Nolfo, Elder Law Section
- Robin Silverman, Intellectual Property Section
- Evan Spelfogel, Labor and Employment Law Section
- Raul Tabora, Health Law Section

Respectfully submitted,

Kelly M. Slavitt and Alison Arden Besunder
Co-Chairs, Task Force on Privacy

Matthew Asbell, Esq.
Ladas & Parry LLP
New York, New York

Michael I. Bernstein, Esq.
Bond, Schoeneck & King LLP
New York, New York

April B. Chang, Esq.
Phillips Lytle LLP
New York, NY 10022

Lauren Fass, Esq.
Arent Fox LLP
New York, New York

Darrell Gay, Esq.
Chair of Employment Law Working Group
Arent Fox LLP
New York, New York

Paul Gillan, Jr., Esq.
Capitol District Physicians Health Plan Inc.
Albany, New York

Lawrence S. Goldman, Esq.
New York, New York

Randy Henrick, Esq.
Associate General Counsel
Dealer Track, Inc.

Jo-Ann Marchica, Esq.
Co-Chair of Health Law Working Group
Arent Fox LLP
New York, New York

Lindsay Martin, Esq.
McKool Smith
New York, New York

Malvina Nathanson, Esq.
Chair of Criminal Law Working Group
New York, New York

Jay G. Safer, Esq.
Co-Chair of Litigation Working Group
Locke Lord Bissell & Liddell LLP
New York, New York

Grace Sterrett, Esq.
Chair of Business Law Working Group
Hudson Cook, LLP
Clifton Park, New York

Wayne Outten, Esq.
Outten & Golden LLP
New York, New York

Arnold Pedowitz, Esq.
Pedowitz & Meister, LLP
New York, New York

Jill Steinberg, Esq.
Co-Chair of Health Law Working Group
Arent Fox LLP

Lake Success, New York

Dennis Lalli, Esq.
Bond, Schoeneck, & King
New York, New York

Mark Mahoney, Esq.
Harrington & Mahoney
Buffalo, New York

Maryrose Maness, Esq.
Warner Music Group
New York, New York

Raymond A. Mantle, Esq.
Neptune Beach, Florida

New York, New York

Oren Warshavsky, Esq.
Baker Hostetler
New York, New York

Miriam Wugmeister, Esq.
Morrison & Foerster
New York, New York

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

THE FORMATION OF THE TASK FORCE

Upon her selection as President-Elect, President Bernice K. Leber began discussing a project regarding privacy. By the time she took office on June 1, 2008, the Privacy Task Force had already been created and a Mission Statement formulated. The members of the Task Force were selected and drawn from practitioners in each of the six fields addressed in the report – criminal law, employment law, health law, intellectual property law, business law, and litigation. The Task Force proceeded to finalize the outline of topics that it would seek to address. On October 9, 2008, the New York State Bar Association issued a press release announcing the creation and mission of the Privacy Task Force.

PURPOSE AND MISSION OF THE TASK FORCE

Protecting lawyers and clients from third-party disclosure of information is a fundamental concern of the legal profession and private citizens. With technological advancement comes an increased risk of illegal and improper disclosure and misuse of personal and business information. From lawyers representing Guantanamo Bay detainees whose computers and telephones were bugged by the government, to lawyers advising individual and business clients on how to meet security vulnerabilities and privacy obligations, these scenarios give rise to a concern about maintaining the American public's expectation of privacy. Daily transactions, communications, and interactions (*e.g.*, sending e-mail on one's computer, providing access to health information or financial or private business information) give rise to potentially severe consequences resulting from possible invasions of privacy or disclosure of confidential or privileged information. One concern is a potential invasion of the attorney-client privilege due to a breach of security in electronic communications and systems and servers, and the impact this has on lawyers, their clients and the public.

The Privacy Initiative has followed its stated mission to identify and select certain

privacy issues impacting lawyers and their clients (both businesses and individuals) in the delineated areas of intellectual property, health and financial information, criminal law, employment law, and litigation. The Task Force reviewed many of the laws, statutes and rules in these areas with the goal of identifying ways to educate the profession (and the public) about the current status of the law with respect to privacy issues and help attorneys counsel their clients who may approach them with a diverse range of privacy-related issues. The Task Force also evaluated the available remedies for violations of privacy laws.

The challenge that the Task Force faced is that this is a vast area of the law that is constantly and rapidly evolving. These laws and the state of the technology that operate in practice are far from static. Accordingly, the broad question the Task Force addressed is: what rights exist to protect personal and private data, and what obligations do individuals and businesses have when collecting, storing, accessing, and using that information? On October 31 and November 1, 2008 Co-Chairs Alison Arden Besunder and Kelly M. Slavitt presented to the Executive Committee and to the House of Delegates on the preliminary findings of the Task Force regarding the legal importance of individual privacy (professional as well as personal) and the topics being explored by the Task Force. These Co-Chairs also presented its Report to the Executive Committee and to the House of Delegates on January 29 and 30, 2009, respectively. Pursuant to the Resolution that was passed at the meeting of the House of Delegates on January 30, 2009, the House of Delegates: (a) acknowledged receipt of the Report as an Interim Report; (b) authorized the Task Force to "complete the study of the issues and further investigate, analyze, discuss and debate the issues raised in the report with the goal of identifying suggestions for reform, if any"; (c) authorized the Task Force to "report back to the House of Delegates concerning the sufficiency of existing law to protect and properly safeguard personal data of

lawyers and their clients in all substantive areas of law including, but not limited to, criminal law, health law, intellectual property, employment law, financial laws and regulations"; and (d) directed the Task Force to report as appropriate "on additional developments in the law on privacy as it affects lawyers and their clients" and report back to the House of Delegates at its regularly scheduled meeting in Albany, New York on April 4, 2009. In accordance with the Resolution, the accompanying Report addresses feedback received during and since the NYSBA Annual Meeting in January 2009, incorporates comments and observations made at the Privacy Summit held on March 5, 2009, and updates certain areas to reflect changes to the law since December 2008.

MISSION STATEMENT

The Task Force was guided by the following Mission Statement:

> Protecting lawyers and clients from third-party disclosure is a fundamental concern of our profession and for citizens alike. As technology has advanced, so does the risk of illegal disclosure and inadvertent misuse of personal and business information – both at home and in the workplace. From lawyers representing Guantanamo Bay detainees whose computers and telephones were bugged by the government, to lawyers advising clients and businesses how to meet security vulnerabilities – there still remains a high expectation of privacy. In the face of daily transactions and events (e.g., sending emails on one's computer, providing access to health information or financial or private business information), the consequences of invasions of privacy are far-reaching, especially considering, among other things, possible invasions of the attorney-client privilege.
>
> The Task Force is charged with identifying discrete areas of privacy for lawyers and those they represent (businesses and individuals) concerning the Internet, health and financial information. The Task Force shall review the laws, statutes and rules in these areas. It shall propose procedural and substantive changes where necessary. The Task Force shall provide opportunities to educate the profession and the public on privacy with the aim of ensuring that our laws, policies and practices are designed to reduce the risk of violations of privacy. In addition, the Task Force shall review and report on the current remedies/compensation available to those whose data have been seized for illegitimate purposes.
>
> The Task Force shall prepare a report which covers the current state of the law and shall recommend any appropriate reforms, both by statute, policy and practice, to the Executive Committee and the House of Delegates.

The following Report satisfies the stated mission by addressing the current state of the law in the six selected delineated areas (health, criminal, employment, litigation, business, and intellectual property) and will serve as a foundation for continued oversight of this area by practitioners, clients, and Association Sections.

MEETINGS OF THE TASK FORCE

The Task Force conducted a series of meetings through telephone conferences between its inception and the printing of this Report. Specifically, the Task Force first conducted a series of conferences between the Summer of 2008 and December 2008, when the Interim Report was

printed. The individual working groups of the Task Force separately conducted their own meetings and collaborated on the drafting of respective chapters of the report. The Task Force conducted an in-person meeting on January 27, 2009 during the NYSBA Annual Meeting, and again at the Privacy Summit on March 5, 2009 (see below). The Task Force also convened on February 25, 2009 and March 11, 2009 to discuss updates to the report for presentation to the House of Delegates on April 4, 2009 and the terms of the Resolution to be proposed to the House of Delegates. The Task Force, through its Co-Chairs, members, and Association liaison, also engaged in concerted efforts to reach out to Association Sections and Committees and select local bar associations to elicit feedback and suggestions on both the Report and the privacy issues addressed therein.

THE PRIVACY SUMMIT

Following the presentation to the NYSBA Executive Committee and House of Delegates at the Annual Meeting in January 2009, the Task Force sought to solicit feedback and input from the various NYSBA Sections and select bar associations. First, the Task Force reissued the Report to all NYSBA Sections in early February 2009 (the Sections had received the Report following the initial mailing on January 5, 2009). Shortly thereafter, the Task Force also sent the Report to local bar associations for review and comment.

On March 5, 2009, the Task Force hosted a Privacy Summit in response to the comments that it received following distribution of the interim report and the meetings of the NYSBA Executive Committee and House of Delegates on January 29 and 30, 2009, respectively. The Task Force invited each Section to appoint two section representatives to attend the Privacy Summit. The Summit sought to facilitate discussion to identify the privacy issues of concern to the Association Sections and elicit opinion and comment about those issues, particularly:

1. The electronic health information system proposed by the Obama administration;

2. Nationalized standard of privacy laws, including data security breach laws;

3. Laws concerning the collection and use of private information;

4. Technological standards for protecting client files and personal information;

The Privacy Summit was attended by approximately twenty people, including members of certain NYSBA Sections as well as representatives from non-Association related public interest groups such as the ACLU. A representative from the Bronx County Bar Association also attended.

Many of the attendees commented on and commended the opportunity to participate in a discussion that convened divergent viewpoints on the important privacy issues discussed. The engaging discussion that occurred at the Privacy Summit resulted in the identification of the following issues as being at the forefront of importance in privacy law today:

1. **Medical Information Technology**: The key issues fall into categories of: (a) agency and government enforcement of privacy regulations for compliance and funding to permit smaller organizations to become compliant without oppressive financial cost; (b) the effectiveness and enforcement of penalties to be imposed for poor or breached security; (c) assistance to covered entities to implement internal controls, including education of medical personnel to ensure proper, secure, and compliant use of information systems; (d) whether there should be private rights of action for breaches of medical security; (e) whether there should be customer / patient access to, verification of, and ability to correct his or her medical records, and whether and to what extent customers / patients should have control over the contents of their database records and the implications of allowing customers / patients to "opt out" of a national medical database; and (f) to what extent information voluntarily submitted to medical databases (e.g., Google Health) should be subject to new privacy protections and regulations that arise out of the recently enacted stimulus legislation.
2. **Employment**: The extent to which an employer may access and use information (both employment and non-employment related) about an employee or potential hire including information about the individual posted on the Internet that cannot be readily verified and material posted on social networking sites.
3. **Record Retention and Destruction**: The disposal, destruction, and maintenance of client files (both paper and electronic) by lawyers and law firms, including whether there should be a "catch all" period for mandatory destruction of all records containing non-public personal information of consumers;

4. **Bankruptcy Issues**: The ability and preconditions to sell private consumer information in bankruptcy proceedings as an asset of the bankruptcy estate (for example, when a privacy notice says that the bankrupt company doesn't share information);
5. **Record Retention Periods**: Whether there should be minimum and/or maximum periods for data retention, with a specific emphasis on data retention requirements for ISP's. Should there be a "catch-all" period for mandatory destruction of all records containing non-public personal information of consumers?;
6. **Social Security Numbers**: The use of Social Security numbers as an identifier for any purpose, with a specific focus on (a) how to prevent future use of Social Security Numbers as common identifiers; (b) how to remedy past and present abuses; (c) what is an appropriate alternative for authenticating identity (e.g., biometric identity cards);
7. **Uniformity in Breach Notification Laws**: Whether there should be a national standard for data breach notification and other privacy laws;
8. **Enforcement and prosecution of data breaches and privacy violations**: How to enforce and prosecute data breaches and privacy violations such that the risk of inadequate data security and privacy violations more than merely a "cost of doing business"; and
9. **Technology Standards**: Whether a baseline can be established as to the minimum level of technological protection an attorney must use in protecting client information and the attorney-client privilege.

These areas were developed as a result of the discussions conducted at the Privacy Summit and were approved by the Task Force members on March 11, 2009 as issues of sufficient importance to warrant further study and analysis.

What the Privacy Task Force has concluded, first and foremost, is that this area of "privacy law" is constantly – and rapidly – evolving. Technology advances at a rapid pace, and the development, passage, and modification of statutory and case law is hard-pressed to keep abreast of such rapidly forming developments. Even as of the writing of this report, recently published articles in the New York Times evidence new developments in this area. The Labor and Employment Section in particular expressed a desire to prepare its own analysis of privacy issues specific to the various constituent groups of that Section, and to reach a consensus among themselves as to issues of import, conclusions and recommendations. It indicated its intention to

do so within the next twelve months and coordinate with any ongoing privacy initiative authorized by the Association. It is for these reasons that the Task Force recommends that the NYSBA continue to maintain oversight over legal and practical developments in this field, and that the NYSBA further the Task Force's stated mission of educating the public by, among other things, offering specific privacy-related CLE programs and coordinating with public interest agencies to offer public-education programs on the existing laws in this field.

EXECUTIVE SUMMARY OF THE REPORT

Updates to the Report

The Report has been updated to reflect the comments received since the Annual Meeting, including comments received at the Privacy Summit. The updates reflect intervening developments in the law since the last report was generated. These updates do not significantly change the Interim Report except to update the Report to address the following:

- The Health Law chapters were updated to address the American Recovery and Reinvestment Act of 2009, which (among other things) expanded HIPAA's application and permit State Attorneys General to bring enforcement actions based on HIPAA violations.
- The Health Law chapters were also updated to address the Health Information Technology for Economic and Clinical Health Act (the "HITECH ACT") pursuant to which the Obama administration has made the expansion of health information technology a major priority.
- The Intellectual Property chapters were updated to include citations to the FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, issued February 2009, revising its Principles related to online behavioral advertising. The Intellectual Property chapters also note the recent controversy caused by Facebook's modification to its Terms of Use such that Facebook deems itself the "owner" of a user's information, even after the user terminates the account. And the chapters updated the information regarding email packets.
- The Business Law chapters have been updated to reflect clarifications regarding applicability of business laws to certain types of businesses, and regarding opt-out rules. It also clarifies rights with respect to receiving free annual credit reports. The Business Law chapters also point out that State Attorneys General have enforcement jurisdiction under FCRA.

- The Employment Law chapters have been updated to reflect clarifications and changes that have been incorporated at the specific request of the Labor and Employment Section, as communicated through the specifically designated Labor and Employment Section representative on the Task Force.
- Remaining portions of the Report were slightly modified to clarify points that some comments indicated were ambiguous or unclear, to correct minor typographical errors or stylistic inconsistencies, and to add newly issued citations.

These updates do not lend themselves to an errata sheet, however, the Task Force will make copies of a "blackline" comparison of the changes available to any Association member upon request.

Summary of Report

- This summary was prepared for the purpose of providing a brief overview of the contents of this Report.
- The Privacy Initiative was commissioned by New York State Bar Association President Bernice K. Leber to examine privacy issues impacting lawyers and their clients, and how to protect against unauthorized collection, use, access, and disclosure of private information, as well as protect organizations that need advice on how to navigate the labyrinthine regulation scheme governing privacy and data security issues.
- President Leber assembled a team of members as a Privacy Task Force Initiative to survey the state of the law affecting issues of privacy and private information.
- The result is the attached Report that highlights components of laws affecting privacy in six key areas: intellectual property, criminal law, health law, employment law, business law, and civil litigation.
- The Report seeks to address issues that affect lawyers, their clients, the legal profession, and the public.

Intellectual Property

- Rapid technological developments have resulted in a massive amount of private information being disseminated, collected, stored, used, and accessible by a wider universe than ever before.
- The advent of technology – especially the Internet, combined with the digitization of content, electronic data storage and sophisticated computer hardware and software sharing common design and operating features and characteristics – has made the protection of privacy a major issue affecting citizens' and residents' personal lives, medical and health records and financial affairs in ways not conceivable ten years ago.
- Identity theft as one form of privacy invasion today is a major risk, especially for people who use the Internet for commercial and financial transactions or for social networking.

- There is an increased collection and use of personal data through technology, including smart and cell phones, GPS units, E-Z Passes, ID badges, surveillance video cameras, WiFi, Internet browsing, credit cards, web site usage and e-commerce purchases, to name but a few.
- All of this collected data has created a field known as "Collective Intelligence": data provided by individuals (willing or otherwise) used by third-parties for purposes ranging from improving the efficiency of advertising to giving community groups new ways to organize.
- Terms of Use and privacy policies on Internet web sites help guide web site hosts and users alike as to the boundaries of how information will be collected, stored, used and shared. Users can also take individual steps to protect against the collection and disclosure of information, such as disabling "cookies", using ad-blocking software, and, of course, taking nominal steps to share less information.
- This section of the Report also addresses "cloud" computing and storage, virtual computing and data storage, and how attorneys may use offshore outsourcing and technology while still preventing against unauthorized access or disclosure of confidential client information.

Criminal Law

- From a criminal law standpoint it has become increasingly difficult to maintain the privacy of personal information because of, among other things, the perceived imperatives of the "war on terror."
- As a society, we are accustomed to having our daily lives recorded, so much so that we are often unaware of and unconcerned with the consequences. Several examples of these intrusions are:
- The E-Z Pass, MetroCard and NEXUS card, cameras at traffic intersections, and surveillance video cameras in ATM machines and high-security locations like Wall Street and airports, all of which result in the recording of information concerning an individual's whereabouts and activities.
- Entry to or travel within public facilities, such as airports, railroad stations, and courthouses, may require passing through a scanning device, searching bags, removing and displaying the contents of pockets, and even removing articles of clothing.
- Recent case law has approved the use by police, without probable cause or reasonable suspicion, of GPS devices affixed to private vehicles to enable the police to track the vehicle's movements.
- Courts have upheld border searches of laptop computers without reasonable suspicion, the search at the border of an envelope containing personal correspondence and found inside another envelope. Such searches place in jeopardy the privacy not only of the traveler, but his or her associates or relatives. Employers of business travelers crossing boarders are vulnerable to the disclosure of confidential business information. Client confidences and privileged attorney-

client information is also vulnerable to such searches.

- The "War on Terror" has generated its own set of privacy invasions. For example, the USA PATRIOT Act expanded the circumstances under which the government can use "National Security Letters" ("NSLs") to obtain information from, *inter alia*, telephone and Internet service providers (including libraries with computer terminals). The *Washington Post* reported in November 2005 that over 30,000 NSLs had been issued each year under the USA PATRIOT Act.

- The USA PATRIOT Act also expanded the ability of the government to obtain court-ordered electronic surveillance. Although previously the Foreign Intelligence Surveillance Act ("FISA") permitted the issuance of a warrant for surveillance of a "foreign power" where "the purpose" of the surveillance was obtaining foreign intelligence, now obtaining foreign intelligence requires only "a significant purpose." Critics contend that this amendment permits the government to carry out electronic surveillance for criminal law enforcement purposes, but without the safeguards (such as demonstrating probable cause to believe the target is involved in criminal activity, strict minimization requirements and post-search notification) contained in the general wiretap statute. The ACLU filed a complaint in the Southern District of New York in July 10, 2008 challenging the constitutionality of FISA amendments.

- Of greater concern to the legal profession are the limitations that the government has imposed on the privacy of attorney-client communications between inmates and their attorneys. Following September 11th, the Bureau of Prisons was given authority to monitor communications between inmates and their attorneys. In addition, detainees at Guantanamo Bay were advised that they were entitled to consult with counsel but that a privilege team would "monitor [and record] oral communications in real time between counsel and the detainee during any meetings" and would "review all written materials brought into or out of the meeting by counsel ...," including notes taken by the attorney during his consultations with his client. These procedures were later rejected by the court.

- The expectation of privacy of one who becomes embroiled in the criminal justice system is necessarily diminished: the police may search a suspect incident to an arrest based on probable cause or pursuant to an arrest warrant; the police may search private premises based on a search warrant; written and oral communications between an individual placed in detention following an arrest and family or friends will be monitored; and jail cells are subject to searches for contraband. A conviction results in more infringements on privacy interests. Even the person placed on probation is subject to search by the probation officer, as is that person's home and possibly place of business. Sex offenders may be required to register on a publicly available registry.

- These limits on privacy are by and large appropriate and justified by the special circumstances. However, sometimes the balance is not struck appropriately. The Second Circuit has struck down the blanket policy of some Police or Corrections Departments to strip search all misdemeanor arrestees, finding that the invasion of privacy was unjustified without particularized suspicion that the arrestee is

concealing contraband.

- As is evident from the remainder of this Report, the very existence of the Internet and other new technologies have changed the landscape and requires a renewed vigilance to ensure that the vastly increased potential for exposure is appropriately controlled and that privacy rights are infringed only for the best of reasons.

Health Law

- This section of the Report summarizes the privacy component of "HIPAA" (the Health Insurance Portability and Accountability Act of 1996), which primarily governs all privacy-related issues concerning patient medical information in all formats. HIPAA remains the most comprehensive and significant body of medical privacy standards in effect today. HIPAA regulations are divided into three parts: (i) privacy standards, (ii) security standards, and (iii) transactional standards. The Report focuses on the privacy standards.
- The Report addresses issues relating to accessing and protecting patient health information and considerations for attorneys in dealing with their clients' health-related information.
- The fundamental information regulated by the HIPAA privacy standards is "protected health information" ("PHI") and the fundamental entities regulated by HIPAA are "covered entities." Physicians, hospitals, and health insurers are "covered entities." With rare exception, entities such as newspapers, police agencies, professional baseball teams, and schools are not.
- HIPAA focuses on two basic activities that can occur with PHI: use and disclosure. Use is any given use - such as analysis, examination, or application - of PHI within the covered entity. Disclosure is the release, transfer, or transmission of PHI, by whatever means, to a party outside of the covered entity. The privacy standards describe the permitted uses and disclosures of PHI in detail. HIPAA prohibits all uses or disclosures of PHI except those that take place as described in, and in accordance with, the privacy standards.
- Although New York lacks a comprehensive statute or regulation comparable to HIPAA to address the privacy and security of patient health information, however, New York State does maintain a patchwork of laws and regulations that: (i) impose obligations on specific classes of providers, such as physicians, hospitals, nursing homes and mental health programs; (ii) set forth enhanced protections for specific types of health information, *e.g.*, HIV information and genetic information; (iii) provide patients and their representatives a right to access their own information; and (iv) address disclosure of medical records and information in the context of litigation. However, HIPAA's preemption provision significantly impacts New York's laws on the privacy and security of health information, overriding some and leaving others intact.
- Last, this section addresses the future of health privacy and whether the existing legal framework is sufficient to address the privacy, security and consent issues that arise with advances in healthcare information technology. Among these developments are (1) the increasing adoption of electronic health records ("EHRs") rather than traditional paper-

based medical records, (2) the growth of e-prescribing; (3) the creation of regional health information organizations ("RHIOs"); and (4) the ultimate goal of a National Health Information Network ("NHIN"). Legislators, regulators, attorneys and healthcare practitioners are increasingly facing the question of how to apply HIPAA and other federal and New York state healthcare laws to these new technological advances.

Employment Law

- This section of the Report analyzes several New York State laws that impact the collection and use of personal information about employees by employers, including, but not limited to: the New York Employee Personal Identifying Law, the New York Disposal of Personal Records Law, and the Information Security Breach and Notification Act.
- For example, the New York Employee Personal Identifying Law (New York General Business Law Section 399-dd; effective on January 3, 2009), prohibits employers from visibly printing on an identification card, publicly posting or displaying, or placing in unrestricted files an employee's Social Security number. The law will also prohibit employers from communicating to the general public an employee's personal identifying information, including a Social Security number, home address or phone number, personal e-mail address or parents' pre-marital surnames.
- Similarly, the New York Disposal of Personal Records Law (New York General Business Law Section 399-h) requires businesses to take certain steps when disposing of business records containing personal information such as shredding the record, destroying the personal information contained in the record, modifying the record to render the personal information inaccessible, or taking action consistent with industry practices to ensure against unauthorized access.
- The Information Security Breach and Notification Act (New York General Business Law Section 899-aa) requires businesses to notify affected customers and the appropriate authorities when an unauthorized party manages to access computerized data containing private information.
- The Report also addresses issues relating to whether and how employers can use information learned about employees based on the employee's "after-hours" activities, including recreational and political activities, blogging, and cigarette smoking.

Business Law

- This section of the Report addresses the various regulations governing privacy in the financial sector.
- One of the primary regulations in this sector, the Gramm-Leach-Bliley Act of 1999 ("GLB"), established a federal standard of privacy that protects individuals in their dealings with entities that provide financial services and products for "consumer" (*i.e.*, personal, family or household) purposes. GLB imposes on each financial institution an "affirmative and continuing obligation" to respect the privacy of its consumers and limits when it can disclose non-public personal information about a consumer to non-affiliated third parties. Among other things,

financial institutions are required to have a written privacy policy describing potential uses of personal information collected. Financial institutions must also implement safeguards to insure the integrity of customer data and protect that data against unauthorized access or disclosure.

- The Report also addresses the adoption by the federal bank agencies of the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" which set forth standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. The Guidelines address standards with respect to the proper disposal of consumer information.
- The Report further addresses the Fair Credit Reporting Act ("FCRA") (15 U.S.C. Section 1681-1681(x)), originally enacted to protect information collected by consumer reporting agencies such as credit bureaus, and the Fair and Accurate Credit Transactions Act ("FACTA"), which implemented amendments to FCRA.
- Finally, the Report addresses the laws dealing with data security and identity theft, including the so-called "Red-Flags" Rule. The discussion includes the State Data Security Breach Notice Law, restricting the use of Social Security numbers, and the New York State Fair Credit Reporting Act, which offers an additional consumer protection by requiring entities to disclose that a consumer report may be ordered in connection with certain kinds of applications before the report is ordered by the user.

Civil Litigation

- The various laws and regulations restricting the collection, management, use and disclosure of private information discussed in the Report are potentially at odds and conflict with the Federal Rules of Civil Procedure, which impose broad discovery obligations on litigants and recipients of subpoenae. The challenge for attorneys and their clients is to balance these competing obligations.
- When responding to a discovery request, all litigants and their lawyers must consider whether there is information in the recipient's possession that constitutes private or personal information and whether that information is governed by privacy laws, some of which are discussed in the Report.
- By way of example, the Report identifies certain privacy laws which permit disclosure in response to a subpoena or court order and others which are silent on the issue. The section offers some suggestions for "best practices" in responding to discovery requests while abiding by privacy regulations.
- The section also addresses potential obstacles presented when the recipient of the discovery request is in possession of information that is housed on a server in a non-U.S. location, or where the U.S. litigant is otherwise subject to penalties in a non-U.S. jurisdiction for disclosure of private information in the U.S.

Concluding Summary

- The Privacy Initiative was tasked with identifying some of the pressing privacy issues

impacting lawyers and their clients (both businesses and individuals) in the areas of intellectual property, health and financial information, criminal law, civil litigation, and employment law. Privacy has become a widespread and constantly evolving field that encompasses nearly all areas of the legal profession. As the Task Force proceeded in its task and research, the members acknowledged the impossibility of addressing each and every aspect of privacy law. The Task Force therefore focused on what its members identified as the most important issues. As was its mission, the Task Force prepared this Report to educate the profession (and the public) on the current status of the law with respect to selected privacy issues. Where applicable, the Report also evaluates the available remedies for violation of the privacy laws addressed. In doing so, this Report provides preliminary answers to the question of what rights exist to protect personal and private data, and what obligations individuals and businesses have when accessing and using information.

- Complete privacy is difficult, if not impossible, to maintain given all the entities that collect, use and store personal information.
- Although technological protections of privacy are available, they are not fool-proof and present challenges to maintain. For example, personal information is divulged both voluntarily and involuntarily in litigation (e.g., discovery requests in employment litigation in particular, in which plaintiff employees routinely seek personnel information concerning co-workers, as well as details of investigations of sexual harassment complaints asserted by other workers claimed to be relevant to liability issues, and employers regularly seek psychological and other medical information concerning plaintiffs in order to defend claims of emotional distress and other damages issues). Carefully crafted protective orders are key in determining who is to be entrusted with personal information, and then monitoring where it ends up.
- This is best demonstrated in the criminal law area, particularly the "war on terror" where perceived imperatives caused an infringement of privacy rights – which must be appropriately controlled to ensure privacy rights are infringed only for the best of reasons.
- As can be seen from this Report, the law is developing to address the challenges raised by technological advances. The role of each lawyer and the legal profession as a whole as advisors to clients is impacted as a result.
- While the existing laws at the federal and state level may be sufficiently comprehensive and broad to address technological issues impacting privacy as it stands today, technology evolves quickly and existing laws need to be constantly evaluated to ensure their sufficiency. In addition, agencies with limited resources should be encouraged to give priority to the enforcement of existing laws. To this end, the Task Force's strongly suggests that the Association continue to examine the sufficiency of the law and its enforcement, maintain oversight of the identified areas of concern, evaluate additional areas of law for examination, seek input from local bar associations and relevant public interest groups, and update this Report regularly on an as-needed basis.

INTRODUCTION

The advent of technology, especially the Internet, combined with the digitization of content, electronic data storage and sophisticated computer hardware and software sharing common design and operating features and characteristics, have made the protection of privacy a major issue affecting personal lives, medical and health records and financial affairs in ways not conceivable as recently as a decade ago. Identity theft is a major risk, especially for people who use the Internet for commercial and financial transactions or for social networking. Surveillance video cameras (which may be combined with facial recognition software) are now ubiquitous in most facilities and areas open to the public and deny us any sense of anonymity. Credit card transactions, E-Z Pass, WiFi, cell phone calls and GPS in cell phones and automobiles record location, activity and movement. The fact that anything published on the Internet can never be recovered or suppressed, even if the original publication was illegal, exposes us all to reduced privacy rights. And the growing use of wireless devices and systems to communicate and transmit content creates a greater risk of interception by unintended recipients.

The digitization of content allows every image, writing and sound, regardless of origin, authenticity or permission, to be copied, appropriated and transmitted globally in a flash to an untold audience. Today the only way to absolutely protect one's privacy is either to not allow any personal content to be recorded on a computer system or in digitized form, or transmitted over the Internet or wirelessly or stored in any database that either might be hacked or from which such personal content might be sent by someone having access or, alternatively, to use secure means to ensure that personal content that has been recorded, transmitted or stored in digitized form cannot be accessed by any unauthorized person (such as by using a secure encryption system). Since even the Pentagon and Department of Defense have experienced unauthorized access to their computer systems and no encryption scheme is entirely immune

from interception, complete protection is both impossible and impractical. Everyone is therefore exposed to the risk that the most private information may become published in a public forum, thereby damaging names and reputations or even finances. Unfortunately, there are no legal or technical means to provide absolute (or even high level) protection against invasion of private information and at best individuals can only hope that their identities remain "under the radar" and thus untargeted.

The history of the legal protection of the right of privacy is long, many faceted, and evolved slowly. Privacy of one's person and home under English law extends back to the Magna Carta and is reflected in the Third, Fourth and Fifth Amendments of the United States Constitution. Privacy of one's name and reputation has long been protected under the law of libel, slander and defamation. As the development of technology and the spreading world of commerce expanded the means by which one's privacy might be invaded or appropriated, the law of privacy has evolved and adapted to fit the new parameters created by photography, phonographs and wire recorders, telegraphs and telephones, radio, television, motion pictures, xerography and other means of recording, publishing and distributing images, sound and information. Over time, new statutes addressing particular privacy issues have been adopted and the courts have adapted the common law to new circumstances and technological means in order to better secure private information.

In 1890, Samuel D. Warren and Louis D. Brandeis published a seminal work in the Harvard Law Review titled "The Right to Privacy,"[1] which cited principles of natural law for their argument that a private cause of action should exist for the publication of truthful, but embarrassing, facts about one's life.[2] Twelve years later, in *Roberson v. Rochester Folding Box*

[1] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy", HARV. L. REV. 193 (1890).
[2] *Id*. at 196.

Company,[3] the New York Court of Appeals held that the plaintiff, whose image was used without permission to sell flour, could not recover for a violation of her right of privacy because no such right existed at that time. In reaction to the *Roberson* decision, the New York legislature enacted New York's first "right of privacy" law in 1903. While this statute was designed to overturn the decision in *Roberson* by providing for recovery of damages for "commercial use type of invasion of privacy," it was not designed to incorporate the broader privacy concepts espoused by Brandeis and Warren. Still, Sections 50 and 51 of New York's Civil Rights Law are the oldest statutes to continuously protect a right of privacy.

Subsequent cases examined using "right of privacy" laws to protect celebrities – who by the nature of their profession are deemed to actively seek public notoriety and acclaim – from commercial exploitation, as opposed to the typical private "right of privacy" plaintiff who just wishes to be left alone.[4] In *Haelan Labs v. Topps Chewing Gum*, Judge Jerome addressed this celebrity/private person difference by coining the term "right of publicity"[5]. The *Haelan Labs* Court considered whether, under New York law, a baseball player could contractually assign the right to produce a card with his image to a baseball card manufacturer.[6] The Second Circuit held that the player's legal right to and interest in his image was assignable and was not limited to merely a personal non-assignable interest or right, as is the case with a right of privacy.[7] In doing so, the Second Circuit considered that

> "in addition to and independent of that right of privacy (which in New York derives from statute), a man has a right in the publicity value of his photograph, *i.e.*, the right to grant the exclusive privilege of publishing his picture [. . .]. This right might be called a 'right of publicity.' For it is common knowledge that

---

3 *Roberson v. Rochester Folding Box Company*, 171 N.Y. 538, 64 N.E. 442 (NY Ct. App. 1902).

4 J. Thomas McCarthy, THE RIGHTS OF PUBLICITY AND PRIVACY at § 1:17 (2d ed. Rev. March 2002).

5 Haelan Labs, Inc. v. Topps Chewing Gum, Inc. 202 F.2d 866 (2d Cir. 1953).

6 *Id.* at 867.

7 *Id* at 868-69.

> many prominent persons (especially actors and ball-players), far from having their feelings bruised through public exposure of their likenesses, would feel sorely deprived if they no longer received money for authorizing advertisements, popularizing their countenances, displayed in newspapers, magazines, busses, trains and subways [. . .]. We think the New York decisions recognize such a right."[8]

Shortly after the *Haelan Labs* decision, Professor Melville B. Nimmer wrote a seminal article on the new right of publicity.[9] Professor Nimmer argued that since the right of privacy focused on protecting one's feelings, it was insufficient to protect the commercial value of one's identity. He also argued that this new "right of publicity" articulated by the *Haelan Labs* decision should be assignable.[10] Thus, according to Nimmer the law should be divided between a property right which could be commercialized (right of publicity) and the right to be left alone (right of privacy).

Professor William Prosser later wrote an article in 1960 categorizing privacy law into four distinctive torts: (i) intrusion; (ii) disclosure; (iii) false light; and (iv) appropriation.[11] In 1977, the Second Restatement of Torts adopted Prosser's four torts as the restatement of the law of privacy.[12]

In the 1970's the New York Courts appeared to recognize a common law right of publicity as well as the statutory right of privacy under Sections 50 and 51 of New York's Civil Rights Law.[13] However, in 1984 the New York Court of Appeals in *Stephano v. News Group Productions,*[14] held that the "right of publicity" is encompassed within Sections 50 and 51 of New York's Civil Rights Law and that there is no common law right of publicity. The New

---

8 *Haelan*, 202 F.2d at 868 (citations omitted).

9 *See* Melville B. Nimmer, the Right of Publicity, 19 LAW & CONTEMP. PROBS. 203 (1954).

10 *Id.* at 203-04.

11 William L. Prosser, Privacy, 48 CAL. L. REV. 383, 389 (1960).

12 RESTATEMENT (SECOND) OF TORTS §§ 652B-E (1977); *see* McCarthy, at § 1:24.

13 See Factors Etc., Inc. v. Pro Arts, Inc. 579 F.2d 215 (2d Cir. 1978).

14 *Stephano v. News Group Productions, Inc.*, 64 N.Y.2d 174, 474 N.E.2d 580 (1984) (male model sued over the unauthorized use in a magazine article of a photograph of him modeling a bomber jacket).

York Court of Appeals stated that although New York's right of privacy statute protected the sentiments, thoughts and feelings of individuals, it was not limited to only these types of cases[15] and that the right of privacy also applied to the unauthorized use of a person's name, portrait or picture for commercial purposes.[16]

In the 1990's the courts further addressed the right of publicity, focusing on whether the right of publicity survives a person's death. In *Pirone v. MacMillan*,[17] Babe Ruth's daughters and heirs sued over the use of their father's image in a calendar. The Second Circuit held that New York's right of privacy protection is limited to living people and does not survive death.[18] In *Orbach v. Hilton Hotels Corp.*[19], the court addressed the fate of the right of publicity when a litigant dies after the action is commenced.[20] The defendant argued that actor Jerry Orbach's New York Civil Rights Law Section 51 claim was extinguished upon his death and his executrix could not continue to maintain the action.[21] The Supreme Court held that because the action had been filed before the actor's death, his executrix could maintain the action in her place.[22]

The "right of publicity" finds its roots in the right of privacy and remains an important legal protection. However, because the right of publicity is distinct from, and has a different focus than, the right of privacy and impacts only a segment of the population (*i.e.*, celebrities), it will not be addressed in this Report.

The following Report addresses select points of interest in order to outline the parameters of the various aspects and implications of the right of privacy today. The Report touches on how the law is developing to address the technological challenges raised, the role of lawyers in

---

15 *Id.* at 182.
16 *Id.* at 183.
17 *Pirone v. MacMillan*, 894 F.2d 579 (2d Cir. 1990).
18 *Id.* at 585.
19 *Orbach v. Hilton Hotels Corp*., 2005 N.Y. Misc. LEXIS 2916 (N.Y. Sup. Ct. July 26, 2005).
20 *Id.* at 6.
21 *Id.* at *4.
22 *Id.* at *6.

dealing with privacy rights both personally and professionally, and, where appropriate, some recommended ways to improve the legal protection of privacy rights. The privacy field is constantly changing today in response to rapid technological developments. Still, it is useful to focus on the issues in an effort to keep both the law and lawyers current and relevant about the law of privacy.

I. INTELLECTUAL PROPERTY LAW CONSIDERATIONS SURROUNDING THE COLLECTION AND USE OF PERSONAL DATA

Personal data is more readily accessible to the general public than ever before. This raises an untold number of issues regarding the collection and use of this information. This Section of the Report will raise questions, answer those questions where possible, and suggest questions and issues to look for in the future.

A. Collection and Use of Personal Data

In 2001, the University of California at Berkeley predicted that, between 2002 and 2005, the world would generate more data than all the data generated on earth during the previous 40,000 years.[23] The seemingly endless reservoir of digital information being recorded by weaving together information from smart phones, GPS units, identification badges, Internet browsing, credit card usage, and web-site information has created a field broadly known as "Collective Intelligence."[24] Collective Intelligence – data provided by individuals, willingly or otherwise – is used by various third parties for improving the efficiency of advertising to giving community groups new ways to organize. As the *New York Times* recently observed:

> But even its practitioners acknowledge that, if misused, collective intelligence tools could create an Orwellian future on a level Big Brother could only dream of.
>
> Collective intelligence could make it possible for insurance companies, for example, to use behavioral data to covertly identify people suffering from a particular disease and deny them insurance coverage. Similarly, the government or law enforcement agencies could identify members of a protest group by tracking social networks revealed by the new technology.[25]

The explosion of personal data used in Collective Intelligence has pushed privacy issues

---

[23] Lyman, Peter and Varian, Hal R, How Much Information?

[24] *See* Group Think, appearing April 4, 2008 on web-site CSV: Comma Separated Values (blog.steinberg.org).

[25] Markoff, John, You're Leaving a Digital Trail. What About Privacy?, New York Times, November 29, 2008.

to the forefront, with nearly every individual and business now potentially impacted by new uses of that data. More than 30 years ago, it was observed that "[t]he real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."[26] That prediction appears to be coming a reality. According to Thomas W. Malone, director of the Massachusetts Institute of Technology Center for Collective Intelligence, "for most of human history, people have lived in small tribes where everything they did was known by everyone they knew … In some sense we're becoming a global village. Privacy may turn out to have become an anomaly." Notwithstanding this prediction, the legal protection of privacy and these data concerns remain at the forefront. The U.S. legal framework regarding privacy and data security issues is continuing to evolve from what started as an industry-specific, ad hoc approach to a more generalized and comprehensive approach based largely on principles of consumer protection.

In considering the intersection between privacy and collective intelligence, we must consider both how information is collected and how it is used – essentially, how Collective Intelligence is created – as well as the issues that arise in connection with both.

1. How Information is Obtained

As one commentator has explained, most of the work on privacy focuses on issues relating to the storage and reuse of data, not the collection of data.[27] Obviously, an individual has significantly less control over his or her personal data once information is in a database: if information never gets collected in the first place, most privacy issues will never arise.

Currently, data is obtained through both voluntary disclosure of information and

[26] U.S. Privacy Protection Study Commission, 1977.

[27] A. Michael Froomkin, The Death of Privacy?, 52 Stanford Law Review 1461 (May 2000).

involuntary collection or even extraction of information. In the Internet context, which is the primary focus here, information is voluntarily disclosed by individuals through registration pages, user surveys, online contests, application forms, and transaction documents. For instance, the use of credit cards in online purchasing allows collection of data about a person's finances, buying habits, etc. Indeed, the continued establishment of loyalty and rewards programs allows for data to be collected about individuals. There are some types of data collection that only the government can undertake, for example, the capture of information on legally mandated forms such as the census, driver's licenses or tax returns. But even these examples illustrate the danger of being too categorical: some states make driver's license data and even photographs available for sale or search, and many tax returns are filed by commercial preparers (or web-based forms), giving a third party access to the data.

Web sites collect both personally identifiable information and data about a user, which may or may not be personally identifiable. Those that collect personally identifiable information can obtain this information in one of several ways:

- the user signs up or otherwise identifies herself to the web site;
- the user identified herself to one web site, and that web site maintains a data-sharing relationship with another web site;
- the user has downloaded software that automatically "reports" back to a web site information about the user's online or offline behavior;
- the user has a unique IP address[28] that can be traced to the particular user.

Voluntary disclosure of information generally includes such seemingly benign pieces of data as name, e-mail address, and possibly the willingness of the consumer to accept e-mails

[28] An "IP" address is the numerical address to which information is sent on your computer.

from the company. In connection with a purchase, a physical address, age range and credit card information are also provided. As further detailed below, this data, which includes personal information about interests, tastes, preferences, purchases, work history, salary, etc., has no inherent expiration, and can be maintained and used for decades.

The fastest growing voluntary disclosure of personal information comes in connection with online social networking, which in recent years has moved from a niche phenomenon to mass adoption. The rapid increase in participation in very recent years has been accompanied by a progressive diversification and sophistication of purposes and usage patterns across a multitude of different sites. Most online networking sites share a core of features: through the site individuals provide a "profile" – a representation of their selves (and, often, of their own social networks) – for others to peruse, with the intention of contacting or being contacted by others (to meet new friends or business associates, find new jobs, receive or provide recommendations, and much more). Individuals are encouraged to reveal information that often revolves around hobbies and interests, but can stride from there in different directions to include anything from semi-public information (such as current and previous schools and employers) to private information, such as relationships, sicknesses, drinking and drug habits and sexual preferences.

Of more concern in the context of privacy is where personal data is collected latently – in a manner often unseen and without an individual's knowledge or explicit consent. Cheap computation makes it easy to collect and process data through keystrokes, monitoring web browsing habits and collection of personalized information. As most people are now aware, web sites may also plant "cookie"[29] files on a visitor's personal computer to gain additional information.

[29] Cookies are "data files created on [users] own computer hard drives when [they] visit a web site [that] contain[s] unique tracking numbers that can be read by the web site." Ann Bartow, Our Data, Ourselves: Privacy, Propertization, and Gender, 34 U.S.F.L. Rev. 633, 678 (2000).

New technologies are employed, without the visitor's knowledge, for companies to record and track information about visitors to their web sites such as e-mail addresses, which portions of the site were visited and for how long, and where the visitors came from. Even without the benefit of high-tech equipment, it is possible for web site administrators to glean information from a user's clickstream – the "aggregation of electronic information generated as a web user communicates with other computers and networks over the Internet."[30] Many sites collect personally identifiable information (such as name, e-mail address or telephone number) directly from the user, though the user may not be aware that such information is being provided. Likewise, sites collect personal information through on-line registrations, mailing lists, surveys, user profiles, and order fulfillment requirements. Another device often used to track user's behavior is a "web beacon" (sometimes called a web bug), which is a miniscule, pixel-sized identifier buried in the software on a page a user views. According to the Privacy Foundation:

> A Web bug is a graphic on a Web page or in an e-mail message designed to monitor who is reading the page or message. Web bugs are often invisible because they are typically only 1-by-1 pixels in size. In many cases, Web bugs are placed on Web pages by third parties interested in collecting data about visitors to those pages.[31]

In short, various devices can be utilized to assist a web site in latently monitoring or collecting data about a user. Although individuals may be aware that portions of this information exist, users often are not made aware of how this information will be stored, shared and/or used. Essentially, reams of data organized into either centralized or distributed databases can have substantial consequences beyond the simple loss of privacy caused by the initial data collection,

---

[30] *See, e.g.*, Adam White Scoville, Clear Signatures, Obscure Signs, 17 Cardozo Arts & Ent. L.J. 345, 364 (1999).

[31] http://www.bugnosis.org/faq.html#web bug basics.

especially when subject to advanced correlative techniques such as data mining.[32] Data accumulation enables the construction of personal data profiles.[33] Personal data profiles and behavioral tracking is the most common use of this data. Among the possible harmful effects are various forms of discrimination, ranging from price discrimination to more invidious sorts of discrimination.[34]

2. How Personal Data is Used

Privacy implications associated with online usage depends on the level of identifiability of the information provided, its possible recipients, and its possible uses. Due to web sites sharing certain information and social networks providing even limited exposure of indicia of personal identification, information about individuals can be collected and correlated. This can be by identifying a profile through previous knowledge of an individual's characteristics or traits, or by inferring previously unknown characteristics or traits about a subject.

To whom may identifiable information be made available? First of all, of course, the information may be made available to the hosting site. It may use and extend the information (both knowingly and unknowingly revealed by the participant) in different ways. Obviously, the information is available within the network itself, whose extension in time (that is, data durability) and space may not be fully known or knowable by the participant. Finally, the ease of joining and extending one's network, and the lack of basic security measures (especially at networking sites) make it easy for third parties to access participants' data without the site's direct collaboration.[35]

---

32 *See* Ann Cavoukian, Info. and Privacy Comm'r/Ontario Data Mining: Staking A Claim On Your Privacy (1998) (quoting Joseph P. Bigus, Data Mining With Neural Networks (1996)).

33 Jerry Kang, Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193, 1202-20 (1998).

34 Oscar H. Gandy, Jr., Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace, 1996 U. CHI. LEGAL F. 77.

35 A. Newitz, Defenses Lacking at Social Network Sites, SecurityFocus, December 31, 2003.

How can that information be used? It depends on the information actually provided – which may, in certain cases, be very extensive and intimate. Risks range from identity theft to online and physical stalking; from embarrassment to price discrimination; and blackmailing. Yet, there are some who believe that such information – especially when used in connection with advanced social networking – can also offer the solution to online privacy problems. In an interview, Tribe.net CEO Mark Pincus noted that "[s]ocial networking has the potential to create an intelligent order in the current chaos by letting you manage how public you make yourself and why and who can contact you."[36]

3. Use of Personal Data and Behavioral Tracking

As illustrated above, the nature of the Internet causes information to pass through dozens of networks and computer systems, each with its own manager capable of capturing and storing online activities. Of particular import, especially when considering the topic of Collective Intelligence, is that user activities can be monitored by individual web sites and Internet Service Providers, vastly increasing the availability of one's personal information to strangers.[37] Collective Intelligence is generally created through the practices of data profiling and data mining.

Data Profiling "is the term used to denote the gathering, assembling, and collating of data about individuals in databases which can be used to identify, segregate, categorize and generally make decisions about individuals known to the decision maker only through their computerized profile."[38] Studies have shown that as many as 92% of all web sites collect personal data of

---

[36] J. Black, The Perils and Promise of Online Schmoozing, BusinessWeek Online, February 20, 2004.

[37] *See, e.g.*, Privacy in Cyberspace, http://www.privacyrights.org/fs/fs18-cyb.htm).

[38] Karl D. Belgum, Who Leads at Half Time?: Three Conflicting Versions of Internet Privacy Policy, 6 Rich.J.L.&Tech. 1, 8 (Symposium 1999).

some sort.[39] Once the data is collected, it is "mined" for information deemed useful to the data collector, such as to construct personal profiles, create targeted marketing and gather other information.[40]

Behavioral Tracking is a technology used by e-advertising companies that can create deep, long-term profiles of online user behavior. In short, it creates advertisements based on user interaction with certain web sites based on the data profiling and data mining. Behavioral Tracking acquires user postings and clickstream data, analyzes that data to form comprehensive personal profiles, and then creates information and advertisements that best match the interests expressed by those profiles.[41]

The Federal Trade Commission ("FTC") defines Behavioral Technology, as "the practice of collecting information about an individual's online activities in order to serve advertisements that are tailored to that individual's interests." The practice involves collecting consumer information that is not personally identifiable in the traditional sense (*i.e.*, by name, address, or similar identifier) and involves sharing of the information with networks that serve advertisements at web sites across the Internet. Currently, there are no legal notice or consent requirements for behavioral tracking; companies are free to monitor web use. The FTC has taken a stance and is pushing towards industry self-regulation. Behavioral Tracking is the most in demand technology; it is utilized by AOL, Google and Microsoft, to name a few.

Recent disclosures of supposedly non-personally identifiable data indicate how easily such information may be linked together to form identifiable profiles of particular individuals.[42]

---

39 *Id.* at 11.

40 A. Michael Froomkin, The Death of Privacy?, 52 Stan. L. Rev. 1461, 1469.

41 *See* FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising (February 2009) revising its Principles relative to online behavioral advertising (available at http://www.ftc.gov).

42 *See* Michael Barbaro & Tom Zeller, Jr., A Face Is Exposed for AOL Searcher No. 44 17749, N.Y. TIMES, Aug. 9, 2006, at Al.

Consider a user who is browsing the Web. As the user surfs the Web, his or her browser retains a history of recently viewed sites. The user can later refer to this list in order to quickly return to these sites. In recent years, several different researchers have discovered methods that allow any web site to discover a user's browser history. These methods include the use of Cascading Style Sheets ("CSS") or JavaScript to query whether particular sites appear in the history file. As a user browses the Web, any marketer or advertising network could use this technique to read the user's entire browser history, and target ads (or do anything else) based on this information.

The legal implications of Behavioral Tracking technology focus around consent and notice. Operating without consumers' knowledge or authorization, Behavioral Tracking technology undermines the ability of users to consent by failing to provide effective notice of its existence. Although only about 1/3 of web sites currently feature Behavioral Tracking, e-advertising consolidation integrates the technology into the world's largest online advertising networks, greatly expanding the reach of user tracking mechanisms.[43]

The Electronic Communications Privacy Act ("ECPA")[44] was enacted to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. While this would be a well understood paradigm for handling behavioral tracking and the like, ECPA has been found inapplicable to possible invasions of privacy by private companies engaging in e-commerce. Specifically, federal courts have refused to hold advertising companies civilly liable for invasions of privacy, instead finding in favor of the defendants.[45] This is an area in the law where change may be needed to ensure greater security

---

[43] *See* Electronic Privacy Information Center ("EPIC"), In re Google, Inc., and Double-Click, Inc., Complaint and Request for Injunction, Request for Investigation and for Other Relief P 30 (Apr. 20, 2007), available at http://www.epic.org/privacy/ftc/google/epic_complaint.pdf.

[44] ECPA Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. § 2510[1].

[45] *See, e.g., In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 502 (S.D.N.Y. 2001); *In re Pharmatrak Inc. Privacy Litig.*, 220 F. Supp. 2d 4, 12-14 (D. Mass. 2002).

and make the entities accountable for the security of information that they collect.

Currently, the FTC is at the forefront of the debate about the use of behavioral tracking. The FTC has made significant efforts to bar spyware and ensure that companies correctly represent security measures via their Terms of Use or Privacy Policies (*See* Section I. B. herein.) Nonetheless, Behavioral Tracking modalities continue to present the unique problem of third parties acquiring information without user consent and without user knowledge. Currently, the FTC has issued a set of guiding principles and appears to be moving toward industry self-regulation. In so doing, the FTC appears to be balancing privacy concerns with the fact that legislation could result in significant loss of income to advertisers, and that Behavioral Tracking can be beneficial for a variety of personal and business reasons. However, self-regulation may not be entirely effective to secure individual rights or agency oversight maybe required to ensure compliance. In this context, it appears that individual security should outweigh any professed business need for "free market" self-regulation given the limited burden imposed on the business.

B. Web sites: Privacy Policy and Terms of Use Considerations

1. Purposes of Terms of Use and Privacy Policy.

Terms of Use ("TOU") policies govern the relationship between the company that owns the web site and the users of the company's web site ("Users") and specifies what the company expects from Users as well as what Users can expect from the company's web site. TOU include information on the web site owner's Privacy Policy, usually as a link. A Privacy Policy is a written description on a specific web site explaining to the public how the company that owns the web site applies specific fair information practices to the collection, use, storage, and

dissemination of personal information provided by Users.[46]

2. Terms of Use

Some companies require Users to explicitly agree to their web site's TOU by checking a box on the web site (a "browsewrap agreement", or a "clickwrap agreement"), while other companies require Users to implicitly agree to the TOU by use of the web site. Courts treat TOUs under traditional contract principles. In a case of first impression in the Second Circuit, *Specht v. Netscape*, the U.S. Court of Appeals applied traditional contract principles to a clickwrap agreement and held that a contract was not entered into between the User and the web site owner.[47] In *Specht*, a web site provided license terms for free downloadable software on the Internet below the "Download" button on the next screen. The web site User claimed to be unaware of the existence of the license terms. The Second Circuit held that a reasonably prudent offeree in the consumer's position would not have known or learned of the reference to the license terms hidden below the "Download" button on the next screen prior to acting on the invitation to download. Therefore, the court held that for a contract to be formed there needs to be conspicuous notice of the existence of the contract terms, and unambiguous manifestation of assent to those terms by consumers.

The benefits of TOU to Users include knowing what is expected of them, while the benefits to companies include the right to deny Users access if they act in a manner that could subject the company to liability (this can be particularly useful to web site owners that post user generated content, "UGC"), specification of governing law, arbitration requirements, and/or forum selection.

TOU must put the user on notice of what they are contracting to. Notice must be

---

[46] *See* also Section IV. herein regarding consent to the disclosure of private information.

[47] *Specht v. Netscape*, 306 F.3d 17 (2d Cir. 2002).

sufficient, so placement and obviousness are most important. TOU are unenforceable if they fail to provide adequate notice of the terms, and there is no showing of actual or constructive use by the User. Knowledge can be imputed based on frequent use where the User saw the TOU each time.[48] "Frequent" has not been defined by the courts.

In order to be effective, web sites should seek to include the following in its TOU:

3. Suggested minimum inclusions for TOU

- *Consent.* Consent language such as "By accessing and using this web site you indicate your acknowledgement and acceptance of these TOU."

- *Intellectual Property Rights.* Reservation of web site owner's copyright and trademark rights, including: statement that all copyrights and trademarks are owned by the web site owner; prohibition on use of content[49]; statement that copyrights and trademarks are protected by federal, state and international laws; and if desired and accurate, statement that the web site owner is a registered agent under The Digital Millennium Copyright Act ("DMCA") so that the web site owner can remove content without liability once notified by a copyright owner that its rights have been infringed, and provide an address for such notice. Some web site owners also include a statement that the use of the company's name/trademark in metatags is prohibited without written consent.[50]

- *Comment Policy (Blogging and UGC).* UGC creates three primary risks: intellectual property risks relating to improper use of another's copyrights, trademarks, or image/likeness; tort risks relating to posting defamatory statements about another; and statutory risks relating to collecting information from children. Protection for web site owners comes from the DMCA, the Communications Decency Act of 1996 ("CDA"), and contract laws applicable to the TOU.

  Early Internet cases regarding liability of service providers for user content[51] were

---

48 *See Register.com v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004); *see also Druyan v. Jagger*, 2007 U.S. Dist. LEXIS 64445 (S.D.N.Y. Aug. 27, 2007)).

49 If any; some web site owners prefer to grant a license as long as certain requirements are met such as their copyright notice and/or trademark not being removed from any content used, while other web site owners prefer to prohibit use without written permission.

50 *See* generally line of cases starting with *Oppedahl & Larson v. Advanced Concepts*, 1998 U.S. Dist. LEXIS 18359 (D.Ct. Colo. 1997) through *N. Am. Med. Corp. v. Axiom Worldwide, Inc.*, 522 F.3d 1211 (11th Cir. 2008); *see* the controversy caused by Facebook recently for updating its TOU (Brian Stetler, "Facebook & Users Ask Who Owns Information", The New York Times, February 17, 2009.

51 *See Stratton Oakmont*, 1997 N.Y. Misc. LEXIS 229, 1995 WL 323710 (holding a service provider liable for speech appearing on its service because it generally reviewed posted content); *Cubby, Inc. v. CompuServe, Inc.*, 776 F.Supp. 135 (S.D.N.Y. 1991) (holding a service provider not liable for posted speech because the provider was simply the conduit through which defamatory

clarified by the immunity granted in Section 230(c) of the CDA[52] precluding courts from entertaining claims that would place a user or provider of an interactive computer service in a publisher's role.[53] In addition, Section 512 of the DMCA creates a "safe harbor" immunity from copyright liability for service providers who "respond expeditiously" to notices claiming they are hosting or linking to infringing materials. To qualify for "safe harbor" protection, the service provider must: have no knowledge of, or financially benefit from, any alleged infringing activity; must have a policy in place to deal with repeat infringers; and must designate an agent to receive copyright complaints.

Web site owners can protect their exposure caused by UGC by including the following:

- posting DMCA information in their Privacy Policy and strictly adhering to what it promises users it will do;
- posting a comprehensive TOU;
- being clear about how it will address information from children;
- post a license for the web site owner to use UGC;[54]
- posting guidelines for acceptable UGC (an example is "Content may not be illegal, obscene, defamatory, threatening, infringing of intellectual property rights, invasive of privacy or otherwise injurious or objectionable."); and

---

statements were distributed).

52 *See* 47 U.S.C. Section 230.

53 *See Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998) (Section 230 immunity applicable where defamatory and harassing message board postings because service provider did not solicit harassing content, encourage others to post it, and had nothing to do with its creation other than through its role as the provider of a generic message board for general discussions); *Batzel v. Smith*, 333 F.3d 1018, 1031 (9th Cir. 2003), cert denied, 541 U.S. 1085 (2004) (the process of an editor selecting which e-mails to publish, and performing minor editing such as spelling, grammar, and length were not "creation" or "development" of information, which would render Section 230 immunity inapplicable); *Carafano v. Metrosplash.com, Inc*. 339 F.3d 1119 (9th Cir. 2003) (postings generated as a result of answers to a host's questionnaires does not make the host an information content provider); *Fair Housing Council of San Fernando Valley v. Roommate.com, LLC*, 521 F.3d 1157, (9th Cir. 2008) (clarifying that immunity under Section 230 does not apply to "development" of information and that a material contribution such as a business entity requiring illegal information from clients as a condition to accepting them as a client qualifies as "development").

54 An example is "By posting or contributing content to this web site, you grant us a non-exclusive, royalty-free, perpetual, worldwide license to use your content in connection with the operation of the services, including without limitation, a license to copy, distribute, transmit, publicly display, publicly perform, reproduce, edit, translate, reformat, create derivative works […..] and/or to incorporate it into a collective work."

- explicitly stating whether its web site will monitor or delete content (some web site owners disclaim any right to review or monitor, some reserve the right to monitor from time-to-time and/or to delete any content posted to the web site, and sometimes with limitations such as if they are solicitations).

- *Liability.* Explicit disclaimer of any warranties, notice that the web site is provided "as is" and at the User's own risk (including as to the web site's security), and a denial of any liability (or a limitation of liability) by the web site's owner. Some web site owners also state that changes to the web site can be done at any time without notice, becomes effective when posted and continued use by the User constitutes acceptance; however, the TOU as well as the Privacy Policy should always be dated when updated to make it clearer for the User, and a more defensible position for the web site owner, which version they previously viewed.[55] A statement that the User's remedy is to discontinue use. Some web site owners require Users to indemnify the web site owner for damages arising from use.

- *Jurisdiction.* What jurisdiction applies, and a statement that the web site is not directed to any jurisdiction where use of the web site is prohibited.

- *Linking to/from*. A sample notification such as: "You acknowledge that when you leave this web site and access a linked site, you do so at your own risk. Links from this web site to third party sites are not an endorsement, authorization, sponsorship or affiliation with this web site or its owner." The specific language varies, with some web site owners not including a statement about third party linking at all, others providing a list of when linking is permitted, and others requiring prior written consent in all cases.

- *Termination.* Right of the web site owner to terminate or restrict access to the User's account for any reason.

- *Information Provided.* Prohibition on Users impersonating another (being anonymous is acceptable), and requirement that Users provide true and complete information about themselves.

- *Prohibition on harassment (on-site and offline).*

- *Technical issues such as the right to store information in the form of cookies.*

- *Security.* Security issues such as: the User being responsible for maintaining the confidentiality of his or her password and for all activities of his or her account; statement that the web site owner can take any action to maintain the security of its web site; prohibition on the User testing the vulnerability of the web site or network to breach access; prohibition on violating the security of the web site by accessing date not intended for the User or by logging onto a server/account the

[55] *See* Discussion, *supra*.

User is not authorized to access; prohibition from interfering with any service to a User such as by submitting a virus, spam or mailbomb; and advisory that e-mail transmissions are not always encrypted.

- *Inclusion of a link to the Privacy Policy.*

4. Privacy Policy

If a web owner posts its representations concerning the use of Personally Identifiable Information ("PII") in a privacy policy, the owner must follow through on that policy or be deemed to engage in an unfair and deceptive business practice.[56] The regulatory bodies for overseeing Privacy Policies are the FTC and the State Attorneys General.

As the federal enforcer of unfair or deceptive acts against consumers,[57] the FTC is the key guardian of online privacy. An act is unfair if the injury it causes or is likely to cause is: (1) substantial; (2) not outweighed by other benefits; and (3) not reasonably avoidable. An act is "deceptive" if it is likely to: (1) mislead consumers; and (2) affect consumers' behavior and decisions about the product or services.[58] Actions brought by the FTC against companies or individuals lead to consent orders and/or negotiated settlements.

The FTC suggests entities that collect and use personal information should adhere to five core principles of privacy protection: notice; choice; access; security; and enforcement.

(1) Notice/awareness as to the company's information practices before any personal information is collected from them so that the consumer can make an informed decision as to whether and to what extent to disclose personal information.

(2) Choice/consent to the consumer as to how any personal information collected from them may be used (such as internal uses like placing a user on the company's mailing list for marketing additional products or promotions, or external uses like the transfer of information to third parties). These are typically opt-in, or opt-out in that they either require the consumer to opt-in

---

56 *See* http://www.cybertelecom.org/privacy/enforce.htm; http://www.ftc.gov/opa/2004/07/gateway.shtm).

57 *See* The Federal Trade Commission Act, 15 U.S.C. § 45(a), Section 5 in particular.

58 Id.

to their personal information being used in such way or opt-out from the company's default position about how the consumer's information will be used unless the consumer tells the company not to.

(3) Access/participation regarding the consumer's ability both to access data about himself or herself and contest its accuracy and completeness.

(4) Integrity/security of the data. The company must take reasonable steps to protect the data's integrity such as using only reliable sources of data and cross-referencing the data against multiple sources, providing consumer access to the data, and destroying untimely data or converting it to anonymous form. Also, the company must take administrative (*i.e.*, internal organizational steps to limit access to data and prevent unauthorized access) and technical measures to protect the data against loss and the unauthorized access, destruction, use, or disclosure of the data.

(5) Enforcement/redress. The core principles of privacy protection are only effective if a mechanism is in place to enforce them, such as a combination of self-regulation, legislation to create private remedies for individuals, and regulatory schemes consisting of civil and criminal sanctions. [59]

The New York State Attorney General's Office has the power both to investigate and to prosecute, through its Bureau of Consumer Frauds and Protection as well as its Internet Bureau, businesses and individuals engaged in fraudulent, misleading, deceptive or illegal trade practices. While consumer protection laws can be found in many statutes, primarily the General Business Law sections, the broadest and most widely used is General Business Law Section 349 prohibiting deceptive and misleading business practices. The key New York State Consumer Protection Laws for handling PII and limiting the potential for identity theft pursuant to the New York State Consumer Protection Board are: New York Social Security Number Protection

[59] *See* FTC 1998 Report to Congress available at http://www.ftc.gov/reports/privacy3/toc.shtm; http://www.ftc.gov/speeches/harbour/06309ipp.pdf (speech of FTC Commissioner Pamela Jones Harbour Before the International Association of Privacy Professionals National Summit, March 10, 2006); *see also* FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising (February 2009) revising its Principles relative to online behavioral advertising (available at http://www.ftc.gov).

Law[60]; New York Employee Personal Identifying Law[61]; New York City Administrative Code[62]; and the Information Security Breach and Notification Act.[63]

Additional protections are required for minors, and these must also be contained in the Privacy Policy. Information about adult activities such as drinking, smoking or pornography must take particular care. If information will be collected from children, the Privacy Policy must specify what kind of information will be collected and how it will be used. The Children's Online Privacy Protection Act[64] ("COPPA") specifically applies to web site operators that knowingly collect personal information from children under 13 years of age.[65] COPPA requires web site operators to:

(1) Post their Privacy Policy on the homepage of the web site and link to the Privacy Policy from every page where personal information is collected;

(2) Provide notice about the information collection practices to parents and obtain verifiable parental consent before collecting such information;

(3) Give parents a choice as to whether their child's personal information will be disclosed to third parties;

(4) Provide parents access to their child's personal information, and the opportunity to review their child's personal information and opt-out of future collection or use of the personal information collected;

(5) Not condition a child's participation in a game, contest or other activity on the child disclosing more personal information that is reasonably necessary to participate in the activity; and

---

60 New York General Business Law Section 399-d and 399-h.

61 New York Labor Law Section 203-d.

62 Section 20-117(g) in conjunction with the Federal Trade Commission's Disposal Rule at 16 C.F.R. Part 682.

63 New York General Business Law Section 899-aa; s*ee* the New York State Consumer Protection Board's Business Privacy Guide available at http://www.nysconsumer.gov/pdf/the_new_york_business_guide_to_privacy.pdf; *see also* Sections V. and IV. herein.

64 15 U.S.C. §§ 6501-6506.

65 15 U.S.C. § 6501, implemented through FTC regulations at 16 C.F.R. Part 312; *see also* Section V. C. herein; *see also* http://www.ftc.gov/coppa

(6) Maintain the confidentiality, security and integrity of personal information collected from children.[66]

COPPA includes a "safe harbor" allowing industry groups and others to request FTC approval of self-regulatory guidelines to govern participating web sites' compliance with the rules above.[67]

5. Recommended Steps for Creating Privacy Policies.

At a minimum, a privacy policy should address the following issues:

a. *What personal information will be collected.* Different areas of a company's web site will likely collect different information, such as e-mail addresses to be added to news alerts regarding loyalty or rewards programs versus credit card numbers to pay for merchandise.

b. *How personal information that is collected can be used.* Some permissible uses are: to process a purchase; to identify new product and service preferences so a consumer can be notified of new offerings that may be of interest; invite a consumer to participate in consumer research; respond to inquiries and/or comments; administer participation in contests; to share it among affiliate/purchaser/third parties with whom a business has a relationship; to share or sell it with anyone (*i.e.*, "We may sell the information you provide to us on this site to a third party or share your personal information.").

c. *How personal information collected be protected.* The FTC brought Complaints against several companies for engaging in the following: storing and transmitting data in clear readable text, storing information indefinitely without a business need; not using readily available security measures to limit access to networks (such as a firewall, and

[66] *See* http://www.ftc.gov/privacy.

[67] *See* samples of FTC enforcement actions at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

protections for wireless access specifically); not encrypting sensitive information consistent with industry standards using algorithms (such as Secure Sockets Layering ("SSL"))[68] rather than a simply alphabetic substitution system; not requiring network administrators to use strong passwords; not requiring users to change user ID and passwords periodically; and failing to suspend user ID and passwords after a certain number of unsuccessful log-in attempts.[69]

d. *Bankruptcy/Merger*. What the company will do with the information gathered if they file for bankruptcy or merge with another company. As one company stated in its policy: "Your information may be transferred as an asset in connection with a merger or sale (including any transfers made as part of insolvency or bankruptcy proceedings."[70]

6. Conclusions/Recommendations on Web sites, TOU and Privacy Policies

Protection of personal information by web site owners is addressed in its TOU and its Privacy Policy. Areas under development include amendments, jurisdictional and enforcement regimes, and technological impact.

---

[68] Note: Transport Layer Security ("TLS") Protocol and its predecessor, Secure Sockets Layer ("SSL"), are cryptographic protocols that provide security and data integrity for communications over TCP/IP networks such as the Internet. Several versions of the protocols are in widespread use in applications like web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP ("VoIP"). TLS and SSL encrypt the datagrams of the Transport Layer protocols in use for an end-to-end connection across the network. TLS is an IETF standards track protocol, last updated in RFC 5246, that was based on the earlier SSL specifications developed by Netscape Corporation. Source: Wikipedia.

[69] *See* http://www.ftc.gov/privacy; other "wrongs" include: not requiring customers to encrypt or protect user ID and passwords; allowing customers to create new user ID and passwords without confirming the new user ID and passwords were created by customers rather than by identity thieves; permitting users to share IDs and passwords; and failing to conduct security investigations to assess their vulnerability such as by patching or updating anti-virus software, or following up on security warnings and intrusion alerts.

[70] *See* http://secondlife.com/corporate/privacy.php; *see also FTC v. Toysmart.com LLC*, 2000 U.S. Dist. LEXIS 21963 (D. Mass. Aug. 21, 2000) (In *Toysmart*, the FTC alleged that a proposed sale of customer information in a bankruptcy proceeding was in direct violation of *Toysmart.com's* Privacy Policy, that stated it would never share the information with third parties. Toysmart.com settled by agreeing to sell only to a similar business that agreed to abide by the original Privacy Policy. Disney eventually purchased the company and destroyed the information.

Once a user agrees to a web site's TOU, if the company amends them it is unclear whether users will be held to those changes by having an affirmative obligation to check for updates each time they access the web site (being on notice that TOU exist on the basis of having agreed to them previously). California caselaw recently held that users are not bound to such a unilateral contract unless given reasonable notice of the change so they can reject the amendments by refusing or terminating the services provided on the web site.[71]

In addition, the law on jurisdiction and enforcement is unclear and many questions remain unanswered. Whose laws apply when a business reaches into another state? Who will enforce individual states' statutes? Various jurisdictions and enforcement regimes leads to a weak incentive for companies to raise awareness of the importance of Privacy Policies in particular. In response, consumers have taken actions to protect themselves, such as disabling cookies, installing ad-blocking software, and sharing less information about themselves.

As technology advances, TOU and Privacy Policies may be difficult to read or can be bypassed entirely. For example, technology such as smartphones and PDAs affect the readability of web sites, and deeplinking (directly to somewhere else on another web site, besides the home page) make it possible to bypass the TOU on the home page.

Web site owners can protect themselves by adhering to the minimum inclusions for their Privacy Policy and their TOU as suggested above. And once stated, web site owners must be careful they adhere to those policies. Web site users can protect themselves by reading the Privacy Policy and TOU for each web site they visit, and knowing what is expected of them. By

---

[71] *See Douglas v. U.S. District Court for the Central District of California and Talk America, Inc.*, 495 F.3d 1062 (9th Cir. 2007) (customer filed class action against long distance telephone service provider alleging violations of the Federal Communications Act and various state law consumer protection statutes, and the customer petitioned for writ of mandamus after the U.S. Dist. Court for the Central District of California granted the provider's motion to compel arbitration under the Federal Arbitration Act).

doing this, both web site owners and web site users are aware of what is expected of them and how their personal information may be used.

C. What Can Be Done to Protect Technology-Based Information

With the expansion of technology, especially Internet and mobile technology in its many forms, lawyers must address the growing privacy issues, including the unintended and unauthorized disclosure of sensitive material, possibly resulting in violations of privacy rights or loss of privileged client information or attorney work product.

For example, lawyers face particularly difficult technical issues in advising clients about compliance with the storage, access, handling and transmission of electronic records subject to discovery. Data stored on media may become inaccessible due to changes in equipment and software without resort to forensic experts and the consequential high cost of recovery. Persons accessing stored data after notice of litigation may inadvertently change the metadata and other technical material raising spoliation of evidence issues. But when and to what degree is an attorney responsible for advising a client about its technology choices and practices and how much technical knowledge must an attorney have to meet his or her professional and ethical obligations, as well as to avoid violation of a person's right of privacy?

In the past, lawyers were not required as part of the fulfillment of and compliance with their professional and ethical responsibilities to master the technical intricacies of technological developments, ranging from the advent of the telegraph, through fax machines and dictation equipment to the Internet. Today, however, lawyers who employ current technology in their practice need to have a sufficient understanding of the technology in order to avoid or properly mitigate the inherent risk that information entrusted to the attorney may become accessible or available to unauthorized persons. To ignore this requirement invites professional malpractice

and ethical violations,[72] especially since attorneys possess information that would never otherwise be disclosed permissibly or intentionally (*e.g.*, in divorce proceedings).

Following are brief descriptions of certain commonly used technology, each of which require understanding by attorneys in order to avoid a privacy or security breach, no matter how closely the attorney thinks he or she is safeguarding the information. The section offers some suggestions of what may (or must) be done to avoid or mitigate this risk.[73]

1. Cloud Computing and Storage, Virtual Computing and Offshore Computing and Data Storage

Use of computer systems in the practice of law has become universal, and today most attorneys have access to a laptop or desktop computer. Some law firms also utilize centralized dedicated computer systems in on-site or off-site server locations. In addition, electronic storage of records has largely replaced paper copies. Remote computing has expanded with the wireless access afforded by WiFi, WiMax, Clearwire and other communication networks to permit access and use of computer systems and data storage while traveling or working outside the office. And Blackberries, smart phones and other wireless PDAs are used to access computer systems and data storage, as well as communicate remotely by text, instant messaging, voice and e-mail.

Cloud computing is a "paradigm in which information is permanently stored in servers on the internet and cached temporarily on clients" such as desktop computers, smartphones, laptops, and potentially any other device connected to the internet at least some of the time (such as a

---

[72] *See, e.g.*, Patricia Wallace, *What Every Attorney Needs to Know About Electronic Technology*, The Florida Bar Journal, Oct. 2008; Richard Ravin, *Use of Wi-Fi Hotspots Can Land You in Hot Water*, Confidential Information at Risk of Lawful Interception, New Jersey Lawyer Magazine, (April 2008 Privacy issue).

[73] It is unacceptable for an attorney to use technology which permits or technically allows or implements unauthorized access and disclosure of privileged client communications, attorney work product or third party information subject to a right of privacy, even if the attorney did not understand or fully comprehend the technical risk involved. As a commercial illustration of this risk, TJ Maxx, Hanaford and other retail stores have incurred substantial penalties and liabilities by using insecure means to transmit credit card data, so that it could be too easily intercepted for criminal purposes (in some cases by persons parked outside the store with a simple wireless receiver).

"dumb terminal", "thin client", or a Blackberry or other mobile device).[74] So-called "cloud computing" (the Internet system itself is often referred to as the "cloud") uses a remotely located computer owned and operated by a third party to enable computing tasks without requiring locally-residing applications. For example, Google offers certain on-line computing applications called Google Apps, and Amazon offers cloud computing of Microsoft Word and other applications at Amazon Web Services. Yahoo, IBM, Microsoft and others also offer cloud computing services.[75] Other popular commercial cloud services and systems include Apple's "MobileMe", a subscription-based service for synchronizing iPhones and certain iPods with desktop computers without a connecting cable and over the internet. "Clouds" behave in such a way that a change in information on one device is automatically made (or "synched") on other devices. For example, with "cloud computing," a change to a person's contact information made on a smartphone is automatically updated on that person's computers at work and at home, as well as any remote server that coordinates the updating.

The risk of "cloud" computing is that because the user usually has no knowledge about the computer's location or even if the same computer is used to perform successive tasks on the same matter, the user has no knowledge of (or control over) the computer itself, the security system protecting physical and electronic access to the computer, the legal system applicable to disputes regarding the privacy and security of information stored on the computer, the persons authorized to access the computer, or the terms of such access. This raises especially potent problems for lawyers, who have both privacy and confidentiality concerns. The global nature of

---

[74] Hewitt, C., "ORGs for scalable, robust, privacy-friendly client cloud computing," IEEE Internet Computing, Vol. 12, No. 5, pp. 96-99, Sep/Oct 2008.

[75] Although it has been suggested that "cloud computing" primarily impacts small or solo law firms, this should not necessarily be assumed given that individual attorneys from any size of firm, company or organization might resort to "cloud computing" because of its cost efficiency or if its usual server fails or is unavailable in foreign locations.

the Internet makes it possible for the "cloud" computers to be anywhere in the world with sufficient network capacity to handle the volume of traffic. Thus, for example, if an attorney uses cloud computing to draft a document on day 1, revises it on day 2 and sends it to the client for review, receives the client's comments, revises it again on day 3 and sends it to the other party or files it with a court or agency, each of the resulting copies on days 1, 2 and 3 could be on a different computer system in a different part of the world and subject to different local laws regarding protection and access of the information on the computer system.

Cloud storage similarly uses a remotely located third-party data storage center which is accessed via the Internet. Cloud storage involves the same type of risks for the data stored on remote servers as cloud computing poses for the material being processed on the computer. To illustrate the scope of one risk, consider that Amazon offers cloud storage through its CloudFront Simple Storage Service, which caches web content in 14 locations in the U.S., Europe and Asia, and Akamai Technologies offers cloud storage on its servers in 70 countries.

Virtual computing involves one computer accessed via the Internet simultaneously functioning as several virtual computers to better utilize the available computing capacity. Put simply, both virtual computing and cloud computing involves shared use of a computer remotely located from the user. If the underlying physical computer is in the law firm's office, then virtual computing may not raise any issue of unauthorized disclosure. But if the physical computer is outside the law firm's office, even if the computer is dedicated to the exclusive use of the law firm, virtual computing still raises some risk of unauthorized access or disclosure. Moreover, if neither the underlying physical computer nor the virtual computer is exclusive, all the same risks are raised as for cloud computing. Indeed from a user's perspective his or her use of a third party remote computer accessed via the Internet may involve both "cloud" computing

and virtual computing with the user having no knowledge of (or control over) either. The issues are becoming even more complicated as so-called public clouds, private clouds and hybrid clouds are evolving to meet market demands.

In addition to the risks posed by cloud computing and storage and by virtual computing, the third party's TOU and Privacy Policy applicable to use of its computer system and data storage must be carefully reviewed to determine if in any way such terms are inconsistent with an attorney's professional and ethical obligations or could lead to disclosure of information in violation of someone's right of privacy.[76] In general, these TOU and Privacy Policies do not afford the necessary level of restriction and protection for privileged client information and attorney work product, or information protected by a right of privacy, so that an attorney professionally and ethically cannot agree to subject such information to those TOU and Privacy Policies. In that case it will be impermissible for an attorney to use cloud computing, cloud storage or virtual computing in his or her practice.[77]

By definition, offshore computing and data storage at a minimum exposes privileged client information, attorney work product and information protected by a right of privacy to a legal system outside the United States and potential access in a manner which may not satisfy New York professional and ethical obligations or comply with applicable law protecting right of privacy. Although ethics opinions have been issued that U.S. attorneys may use non-U.S. offshore lawyers and paralegals to perform services for clients of the U.S. lawyer,[78] the U.S. attorney remains responsible to his or her clients both for the services performed offshore and for

---

[76] *See* Section I.B. herein.

[77] There are numerous technical issues which must be considered in use of cloud computing and storage beyond the protection of information addressed in this Report. *See, e.g.,* How to Plug Into the Cloud, Information Week, Dec. 8, 2008, pp.20-30.

[78] The Association of the Bar of the City of New York Committee on Professional and Judicial Ethics, Formal Opinion 2006-3 (August 2006); Los Angeles County Bar Association Professional Responsibility and Ethics Committee, Opinion No. 518 (June 19, 2006).

the risk of unauthorized access, use or disclosure of privileged client information, attorney work product and information protected by a right of privacy posed by use of the offshore service, including the offshore computer systems and data storage used in connection with such offshore services. Although there are not any rulings specifically about use of offshore computer and data storage systems, the ethics rulings on use of offshore lawyers and paralegals do include an admonition about maintenance of client confidentiality. Accordingly, a U.S. lawyer may not delegate to an offshore person or entity his or her responsibility regarding the risks posed by use of offshore computer systems and data storage any more than the U.S. lawyer can shift responsibility for legal services performed offshore.

Although universal encryption of all documents and other data stored offshore or created or modified via cloud computing, virtual computing or offshore computing would afford reasonable security so that privileged client information, attorney work product and protected PII would not be accessible to unauthorized persons, today universal encryption is impractical because of the additional time required and the resulting delay and expense to encrypt and decrypt the material. Microsoft and RSA (the security division of EMC) are working on a data loss prevention technology to use a combination of encryption, content analysis and role-based access controls to secure computer data while it is in use, while it moves across networks and while it is stored. Until such a data loss prevention system is available as part of an operating system that seamlessly and automatically provides this security, we see no practical means to assure that information on any computer or data storage system neither located in the United States nor dedicated to an attorney's exclusive use may not be accessed by, or disclosed to, unauthorized persons in violation of an attorney's professional and ethical obligations.

2. Border Crossing

Although not a technology issue per se, crossing an international border with a laptop,

Blackberry, smart phone, digital camera, USB thumbdrive, and other device using electronic storage has become a major concern for protection of privileged client information, attorney work product and right of privacy information. While the Fourth Amendment limits all such information from unreasonable search and seizure within the United States, this Fourth Amendment restriction does not apply when entering the U.S. from abroad. Instead, entering the U.S. from abroad permits the U.S. Customs Service to access and review all of the information stored in such devices, without substantial limitation, and if any of the information is determined to be unlawful (such as child pornography), the traveler will be arrested and charged. There is no real exception for privileged client information, attorney work product and protected personal information, so an attorney in possession of any such information who will be entering the U.S. from abroad should not store the information on any such device in order to prevent its disclosure. Instead, the information should be transmitted in a manner not subject to such border search in order to maintain the required client confidentiality, as discussed below. In general, the same rule will apply to travel from the U.S. to another country. Note that any information learned by the U.S. Customs Service through review of the contents of any electronic memory reviewed in connection with a border crossing may be used by the U.S. Customs Service (and related other agencies, such as the Department of Justice) in connection with any investigation or government action, free from the limitations which would apply to a search in violation of the Fourth Amendment.

Subject to export restrictions on sending certain types of information and material from the U.S., to avoid the risk of disclosure of information stored in the memory of a device the information should be sent to a secure party in the U.S. or in the country of destination outside the U.S. (depending in which direction the attorney is traveling) or put in a mailbox, in either

event so the information can be accessed remotely once the attorney has arrived at his or her destination. Although not mandatory, it is recommended that information transmitted abroad electronically be encrypted to add a level of protection. The memory of the device should then be erased, so there will be nothing in the memory to be reviewed by a customs agent when the border is crossed. There are "virtual shredding" software programs available on the market that give better security when deleting such files.

3. USB Thumb Drives

Flash storage permits the storage and transport of digitized data at a minimal cost and with a convenience that increasingly makes it possible for large amounts of data to be stored in a device no larger than one's thumb. This poses two major risks for lawyers. First, because of its small size the device may be misplaced or lost, with all of the stored data becoming available and accessible to an unauthorized person. Encryption of the data can minimize this risk, but the fact is few persons routinely encrypt data which is being stored on a device for future access and use. Secondly, encryption takes more memory, so it limits the storage capacity of the device. Lastly, some types of data (such as visual images) are more difficult to encrypt.

The second major risk is that a USB thumbdrive with downloaded data from one's computer system can be removed from the site, with little record of the event or opportunity to intercept the device's removal. Thus, the ease of use and portability of the device may encourage violation of security policies restricting the copying, transmission or removal of certain types of information, with the resulting risk of loss or other unauthorized access and disclosure of the data. Indeed, to avoid this risk some companies have actually plugged all of their computers' USB ports with epoxy to insure thumbdrive devices cannot be used.

4. Metadata

Although metadata is not per se related to right of privacy information, we have included

this brief description as an illustration of how technology can impose on attorneys an obligation to learn how the technology may result in unauthorized disclosure of privileged client information or attorney work product and thus make it mandatory that attorneys employ appropriate means to avoid such risk of inadvertent disclosure. A similar duty also will apply to right of privacy information entrusted to an attorney, so it behooves attorneys using technology to become informed about the technology in order to avoid inadvertent disclosure of such information.

Metadata is computer generated "information about a particular data set (such as a document) which describes how, when and by whom it was collected, created, accessed or modified and how it is formatted".[79] In other words, it is information about other information. It exists, in general, to provide context to the primary information.[80] Because metadata is computer generated, it is part of every document on a computer system and, under the Federal Rules, is subject to discovery. However, note that some metadata may contain privileged communications or information. Accordingly, an attorney electronically sending a document to anyone other than a co-counsel or client must take appropriate steps to scrub any metadata which contains either privileged client information or attorney work product.[81] Under NY Ethics Opinion 782 (2004), New York lawyers have an ethical duty to use reasonable care when transmitting documents by e-mail to prevent disclosure of metadata containing client confidences or secrets.[82] There are several software programs which may be used to scrub metadata before transmitting documents.

---

79 The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, www.thesedonaconference.org/content.

80 In a computational context, metadata may be actively or passively created. Actively created metadata includes filenames and star ratings for music files. Passively created metadata includes things such as date stamps, filename extensions (e.g., .doc, .pdf), email header contents, and often information about a file's creator, taken from the person's log-in information.

81 Campbell C. Steele, Attorneys Beware: Metadata's Impact on Privilege, Work Product and the Ethical Rules, 35. U. Mem. L. Rev.911 (2005).

82 *See also* Proposed Advisory Opinion 06-2, Professional Ethics of the Florida Bar, June 23, 2006; N.J. Advisory Committee on Professional Ethics Opinion 701, 184 NJLJ 171 (April 10, 2006).

Some New York City law firms routinely use such software, but this seems to be the exception. One can also print a document and scan it back into the computer system, with the scanned copy then sent free of all metadata.

5. Electronic Mail and Messaging

Written communications between attorneys and their clients are frequently accomplished through electronic means, such as electronic mail (aka "e-mail"), instant messaging, and text messaging in various forms.

Probably the most ubiquitous form of electronic written communication today is e-mail. Many might agree that e-mail has replaced the written letter almost entirely. Interestingly, the rise of text messaging, instant messaging, social networking, and related online applications may now be reducing the extent to which individuals rely on e-mail. Still, attorneys continue to use e-mail extensively to advise their clients, and it appears to have been endorsed by ethics decisions.[83] Despite the nearly universal acceptance of e-mail as a means of attorney-client communication, few attorneys likely understand the technology behind e-mail communications or the inherent risks of interception in the absence of certain precautions.

Unlike standard (non-VoIP) telephones or facsimile machines which transmit their signals in their entirety via a temporarily dedicated path from the origin to the recipient, e-mail communications are fragmented into so-called packets by the sender's e-mail provider, and each packet is transmitted over a different path until it reaches the recipient's e-mail provider, where the packets are reassembled. Aside from containing part of the content of the e-mail message, each packet has a header which includes, *inter alia*, the sender's Internet protocol (or "IP") address, which can be used to uniquely identify them.[84] Additionally, some privacy

[83] Ethics Opinion, Association of the Bar of the City of New York NYCPR.
[84] NYCPR.

professionals argue that IP addresses should be considered part of the personally identifiable information that may be protected under privacy laws. More significant privacy-related problems may arise at vulnerable points in the path between the sender's computer and the sender's e-mail provider, especially if either party is utilizing an unsecured wireless network to transmit or receive the message from/on his or her home computer to/from the e-mail provider on the Internet. It is, however, fairly simple to encrypt the message and the headers in outgoing e-mails using cryptography. Recommended standards for encrypting e-mails include PGP, SSL, and WPA for wireless networks.[85] Moreover, an attorney can assure his or her client that his or her message is not forged and has not been altered by using a "Digital Signature". In the event that a third party does obtain unauthorized access to confidential communications over e-mail, civil liabilities may be available under ECPA,[86] and at least according to one commentator, under a theory of infringement of a potentially dormant common law copyright.[87]

Further means of electronic written communications are instant messaging and text messaging (aka "SMS" or "texting"), which are distinct from e-mail in that they can have the immediacy of a telephone call. Most instant messaging services are unencrypted, leading to the increased possibility that communications may be intercepted. Additionally, similar to the issues surrounding cloud computing, the terms and conditions of certain providers of instant and text messaging services can determine whether third parties have access to communications. For instance, the American On-line Instant Messenger TOU states that "AOL is not required to pre-screen Content available on the AIM Products, including the content of any messaging that occurs on or through the AIM service, although AOL reserves the right to do so in its sole

---

85 www.EmailPrivacy.Info; Richard Ravin, "Use of Wi-Fi Hotspots Can Land You in Hot Water, Confidential Information at Risk of Lawful Interception", New Jersey Lawyer Magazine, (April 2008 Privacy issue).

86 ECPA Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. § 2510[1].

87 Ned Snow, A Copyright Conundrum.

discretion". Similarly, in the virtual world called Second Life, the terms of service advise that the proprietor "Linden Lab, in its sole discretion, may track, record, observe or follow any and all of your interactions within the Service." Moreover, a number of messaging services retain the messages for indefinite periods, and thus could be required to produce the communications as a result of a subpoena. Accordingly, it is not advisable to communicate with clients or give legal advice using instant or text messenger applications. However, certain anonymous text messaging services are available, such as AnonTxt.com, which lists among its TOU that "the Site will NOT alter or monitor any text messages".

In addition, attorneys must take precaution to retain certain written electronic communications that the client has a presumptive right to obtain, and they should organize those stored communications to facilitate their later retrieval.[88] Communications that should be retained include formal, carefully drafted e-mail communications intended to transmit information, or other electronic documents, necessary to effectively represent a client, or documents that the client may reasonably expect the lawyer to preserve. Although more casual e-mails may be deleted, it may be advisable to retain even these as a measure to protect against a malpractice claim. Suggested means for organizing retained e-mails include moving those e-mails to an electronic file devoted to a specific representation, and/or coding those e-mails with specific identifying characteristics, such as a client and matter number, when the e-mails are first sent or received.

[88] Ethics Opinion, Association of the Bar of the City of New York.

II. KEY PRIVACY ISSUES IN CRIMINAL LAW

It has become more and more difficult to maintain the privacy of personal information because of new technological developments and the perceived imperatives of the "war on terror." This discussion will highlight some of the major areas of concern and the state of the law with respect to some of these areas.

A. People are Under Constant Surveillance While Traveling About, Whether by the Government or Private Entities

As a society, we have become accustomed to having our comings and going recorded as we go about our daily lives. The use of transportation devices to speed travel, such as the E-Z Pass, MetroCard and NEXUS card, results in the recording of information concerning individual whereabouts. New York City and other municipalities have installed cameras at traffic intersections and the like, purportedly to assist in the enforcement of traffic laws. These cameras record information about one's whereabouts and the whereabouts of one's vehicle. Many private commercial buildings require visitors to sign in and provide photo identification; some even take their own photograph that may be filed away in a computer. It may also be necessary to pass through scanning equipment, especially in locations considered particularly vulnerable to terrorist attack, such as religious institutions or government buildings. Many private commercial and residential buildings use video surveillance equipment. Scanning and inspection of personal property also occurs at public sporting and other entertainment events.

In one instance, at least, the privacy invasion has been sanctioned by the courts. Entry to or travel within public facilities, such as airports, railroad stations, and courthouses, may require passing through a scanning device, opening one's bags, removing and displaying the contents of one's pockets, and even removing articles of clothing. Applying the "special needs" doctrine, the courts have justified random searches of bags and other containers in the New York subway

system, *MacWade v. Kelly*,[89] and of commuter ferry passengers traveling from Vermont to New York, *Cassidy v. Chertoff.*[90]

Some of the technological invasions of our privacy are less well known. In the early 1970's, at the instance of the National Transportation Safety Board ("NTSB"), some automobile manufacturers added electronic sensors and recording equipment on certain air-bag-equipped vehicles that would provide information concerning crashes. Throughout the next years, these electronic sensors were made capable of collecting more and more information and were installed on more and more cars. These "black boxes" sort pre-and post-crash data, such as vehicle speed, brake status, throttle position and the state of the driver's seat belt switch.[91] Subsequently, the NTSB ruled that electronic data recorders would be required in all new cars manufactured in the United States. This ruling met with protests by privacy experts.[92] Perhaps as a result, the National Highway Traffic and Safety Administration ("NHTSA") ruled that "black boxes" would not be required, although they were permitted, and that car makers must tell automobile buyers if such technology is installed in their cars. Further, according to NHTSA spokesman Rae Tyson, recorder information cannot be downloaded without the owner's permission.[93]

The *Wall Street Journal* recently reported that the Department of Homeland Security is beginning implementation of a surveillance program using satellites, despite a report by the Government Accountability Office citing gaps in privacy protection. New legislation purports to

---

89 *MacWade v. Kelly*, 460 F.3d 260 (2d Cir. 2006).

90 *Cassidy v. Chertoff*, 471 F.3d 67 (2d Cir. 2006).

91 Perry Zucker, "Automobile Black Boxes," http://www.expertlaw.com/library/accidents/auto_black_boxes.html (August 2003).

92 Kelley Beaucar Viahos, "Privacy Experts Shun Black Boxes," http://www.foxnews.com/story/0,2933,132056,00.html (September 10, 2004); Mike Adams, "Vehicle black boxes to be required on all automobiles manufactured in the United States," http://www.naturalnews.com/002356.html (November 11, 2004).

93 David Crawley, "US rules on big brother black boxes (Automobiles)." http://www.freerepublic.com/focus/f-news/1688456/posts (August 22, 2006).

focus the program on "emergency response and scientific needs," precluding use for homeland security or law enforcement unless additional safeguards are adopted.[94]

B. The Targeting of Individuals Has Become More Extensive, With the Approval of the Courts.

Recent case law has approved the use by police, without probable cause or reasonable suspicion, of GPS devices affixed to private vehicles to enable the police to track the vehicle's movements.[95]

Courts have upheld border searches of laptop computers without reasonable suspicion, rejecting arguments that the computers store personal information about one's thoughts and memories.[96] A court also upheld the search at the border of an envelope containing personal correspondence and found inside another envelope.[97]

Such searches place in jeopardy the privacy not only of the traveler but his or her associates or relatives. Employers of business travelers crossing borders are vulnerable to the disclosure of confidential business information. Client confidences and privileged attorney-client information is also vulnerable.

The authority granted to the government to issue "administrative" subpoenas to banks, telephone companies, and the like, in connection with the investigation of individuals has been substantially expanded by the USA PATRIOT Act, adopted as part of the "War on Terror."

C. The "War on Terror" Has Generated its Own Set of Privacy Invasions

1. National Security Letters and Other Administrative Subpoena

The government has had the right to use "National Security Letters" ("NSLs") since

---

94 Siobhan Gorman, "Satellite-Surveillance Program to Begin Despite Privacy Concerns," *Wall Street Journal Online*, October 1, 2008 (http://online.wsj.com/article/SB122282336428992785.html?md=go).

95 *People v. Weaver*, 52 A.D.3d 138 (3d Dept.), lv. to appeal granted, 10 N.Y.3d 966 (2008).

96 *E.g., United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008).

97 *United States v. Seljan*, F.3d, 2008 WL 4661700 (9th Cir 2008) (en banc).

1986, but the USA PATRIOT Act expanded the circumstances under which such letters can be issued. The FBI may now request from telephone and Internet service providers (including libraries with computer terminals) "subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession" as long as it certifies that the information is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." The FBI's authority is limited only in that the investigation cannot be conducted "solely" on the basis of First Amendment-protected activities.[98]

The legislation has resulted in a massive increase in the issuance of NSLs. The *Washington Post* reported in November 2005 that over 30,000 NSLs had been issued each year under the USA PATRIOT Act.[99]

Another provision of the USA PATRIOT Act authorizes the government to obtain a court order obligating custodians (including educational or financial institutions, Internet service providers and librarians) to provide records based on the government's certification.[100] Under a predecessor statute, the government was entitled to obtain such a court order on the basis of specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or agent of a foreign power. The USA PATRIOT Act expanded the records that could be sought (any type of record or tangible thing) and eliminated the need to show individualized suspicion. Now, a highly placed designee of the FBI Director need only certify that he or she believes that information relevant to an investigation against "international

---

98 *See* 18 U.S.C. § 2709.

99 Barton Gellman, "The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans," *Washington Post*, Nov. 6, 2005, at A01; s*ee* generally, Susan H. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment," 41 *Harvard Civil Rights-Civil Liberties Law Review* 67, 86-92 (2006).

100 50 U.S.C. § 1861.

terrorism or clandestine intelligence activities" may be obtained (subject to the exception that the investigation cannot be conducted "solely" on the basis of First Amendment-protected activities).[101]

Litigation has challenged aspects of this legislation, in particular the "gag rule" – proscribing a recipient of an NSL or of a court order from disclosing its existence to anybody.[102] While a consolidated appeal from these decisions was pending, amendments to the USA PATRIOT Act in 2006 replaced the prohibition on disclosure with a provision allowing the FBI to review the need for non-disclosure on a case-by-case basis and providing some judicial review. The Second Circuit remanded the Southern District of New York case to determine the issues based on the revised USA PATRIOT Act and dismissed the government's appeal from the District of Connecticut's decision as moot.[103] On remand, the Southern District found portions of the amended statute unconstitutional and not severable and so held the statue unconstitutional in its entirety.[104] On appeal, the Second Circuit agreed that the "challenged statutes do not comply with the First Amendment" but "not to the extent" found by the District Court, and reversed in part because the relief ordered was too broad.[105]

2. Treasury Department Surveillance

One area of administrative subpoenae worthy of separate mention is that undertaken by the Treasury Department under its Terrorist Finance Tracking Program ("TFTP"). It was

---

101 *See* "The USA PATRIOT Act and the Submajoritarian Fourth Amendment," *supra*, at 75-86.

102 *See Doe v. Gonzales*, 386 F. Supp. 2d 66 (D.Conn. 2005); *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004) (asserting First, Fourth and Fifth Amendment claims).

103 *Doe v. Gonzales*, 449 F.3d 415, 419, 421 (2d Cir. 2006).

104 500 F. Supp. 2d 379, 425 (S.D.N.Y. 2007).

105 *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2008); *see also Muslim Community Ass'n of Ann Arbor v. Ashcroft*, 459 F. Supp. 2d 592 (E.D. Mich. 2006) (challenging the statute on First and Fifth Amendment grounds); *see also* Christopher Dunn, "*Kelly v. Mukasey* Letter Exchange: NYPD Surveillance Run Amok?", New York Law Journal, December 22, 2008, p. 3 (discussing the use by the New York Police Department of National Security Letters pursuant to authority granted by the United States Attorney General).

revealed in June 2006 that the Treasury Department served administrative subpoena on the Society for Worldwide Interbank Financial Telecommunications ("SWIFT"), which transmits bank transaction information, for personal data held on SWIFT's United States server. It has been estimated that SWIFT handles 80% of the worldwide traffic for electronic value transfers. Due to questions raised about the legality of these subpoena under European data protection law, the Council of the European Union obtained representations from the Treasury Department and SWIFT concerning the gathering and use of this information and oversight mechanisms. Among other things, TFTP has assured that it will use the information only for counterterrorism purposes and will protect the privacy of persons not connected with terrorism or its financing and that the searches will be limited to pre-existing terrorism investigations and include minimization procedures.[106]

3. NSA Surveillance

According to news reports, President Bush authorized the warrantless surveillance of purely domestic communications by the National Security Agency ("NSA").[107] It has been alleged that the NSA listened in on conversations between two Washington-based attorneys for

---

106 *See* Council of the European Union, "Processing and protection of personal data subpoenaed by the Treasury Department from the U.S. based operation center of the Society for Worldwide Interbank Financial Telecommunication (SWIFT)," 11291/2/07 REV 2 (Presse 157); Federal Register Vol. 72, No. 204, October 23, 2007, p. 60055; The United States Mission to the European Union, "U.S., EU Reach Agreement on SWIFT Terrorist Finance Data," http://useu.usmission.gov/Dossiers/Terrorist_Financing/Jun2907_SWIFT_Deal.asp (June 29, 2007); Eric Lichtblau and James Riesen, "Bank Data is Sifted by U.S. in Secret to Block Terror," New York Times, June 23, 2006, http://www.nytimes.com/2006/06/23/washington/23intel.html?ex=1308715200&en=168d...; "Swift Unlawfully Transfers Personal Data to the U.S.," http://www.hg.org/articles/article_1780.html (December 29, 2006).

107 James Risen and Eric Lichtblau, "Early Test for Obama on Domestic Spying Views," *The New York Times*, November 18, 2008 (http://www.nytimes.com/2008/11/18/washington/18nsa.html?%2359;).; "Exclusive: Inside Account of U.S. Eavesdropping on Americans," *Frontline: ABC News*, October 9, 2008 (http://abcnews.go.com/Blotter/story?id=5987804&page=1); Jonathan S. Landay, "Did US Government Snoop on Americans' Phone Calls?", October 9, 2008 (http://www.truthout.org/101008J); Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA TODAY*, May 11, 2006, at A1).

an Islamic charity, the Al-Haramain Islamic Foundation while carrying out an NSA wiretap of members of that organization.[108] Lawsuits were filed in Detroit and New York challenging this program.[109] In one of the two cases referenced, *American Civil Liberties Union v. National Security Agency*,[110] the district court held that the program, Terrorist Surveillance Program ("TSP"), was unconstitutional and enjoined the government from eavesdropping without a warrant. This ruling was reversed by the Sixth Circuit, which held that the plaintiffs lacked standing because they could not prove they were the targets of TSP.[111]

4. Expanded FISA Wiretapping

The USA PATRIOT Act expanded the ability of the government to obtain electronic surveillance from a specially constituted court by amending the Foreign Intelligence Surveillance Act ("FISA"). The previous version permitted the FISA court to issue a warrant for surveillance of a "foreign power"[112] where "the purpose" of the surveillance was obtaining foreign intelligence. Under the amendment, obtaining foreign intelligence need only be "a significant purpose."[113] Critics contend that this amendment permits the government to carry out electronic surveillance for criminal law enforcement purposes, but without the safeguards (such as demonstrating probable cause to believe the target is involved in criminal activity, strict minimization requirements and post-search notification) contained in the general wiretap statute.[114]

---

108 *See* "Early Test for Obama on Domestic Spying Views"; s*ee also Al-Haramain Islamic Foundation v. Bush*, 507 F.3d 1190 (9th Cir. 2007) for a general discussion about NSA's wiretapping program.

109 *See* "Two Lawsuits challenge Eavesdropping Program," USA Today, January 17, 2006, http://www.usatoday.com/news/washington/2006-01-17-aclu-nsa_x ....

110 American Civil Liberties Union v. National Sec. Agency, 438 F.Supp.2d 754 (E.D. Mich. 2006).

111 493 F.3d 644 (6th Cir. 2007).

112 Defined in 50 U.S.C. § 1801 to include a "group engaged in international terrorism or activities in preparation therefor" or "a foreign-based political organization, not substantially composed of United States persons" as well as foreign governments.

113 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B).

114 18 U.S.C. §§ 2510-2522 (referred to as Title III). *See* William C. Banks, "And the Wall Came

On July 10, 2008, the ACLU filed a complaint in the Southern District of New York challenging the constitutionality of FISA amendments which, the complaint alleged, "allow[] the executive branch sweeping and virtually unregulated authority to monitor the international communications – and in some cases the purely domestic communications – of law-abiding U.S. citizens and residents."[115] As of the writing of this Report there has been no final judgment in this lawsuit.

5. "Sneak and Peek" Authority

The USA PATRIOT Act also expanded the reach of federal authority in Fourth Amendment searches not connected to terrorism investigations by permitting the government to delay notification of the target of a warrant-based search or seizure indefinitely upon a showing that "an adverse result" might occur.[116] Apparently this statute has been invoked primarily in drug investigations.[117]

D. The Government Has Imposed Limitations on the Privacy of Attorney-Client Communications

On October 30, 2001, the Bureau of Prisons was authorized by the Justice Department to monitor communications between inmates and their attorneys. The procedures were engrafted onto an existing regulation that provided for "special administrative measures," or SAMs, to protect against violence in the prisons, and included provisions for administrative segregation

---

Tumbling Down: Secret Surveillance After the Terror," *57 U. Miami L. Rev.* 1147, 1150 (2003). *See In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002), upholding the constitutionality of the amendment and containing a discussion of the comparison between Title III searches and FISA searches.

115 *See Amnesty Int'l USA, et al. v. McConnell, et al*., 108-CV-6259 (JGK) (legal documents in the case available at http://www.aclu.org/salefree/nsaspying/35945res20080710.html). *See* Tom Burghardt, "America's Spying Telecoms: ACLU Challenges FISA Law in Federal Court," 9/18/2008, http://www.globalresearch.ca/index.php?context=viewArticle&cod. For a discussion of the current FISA provisions, see "The USA PATRIOT Act and the Submajoritarian Fourth Amendment," *supra*, at 92-99.

116 18 U.S.C. § 3103a.

117 *See* "The USA PATRIOT Act and the Submajoritarian Fourth Amendment," *supra*, at 100, and n.207.

and the like.[118] Under the new provision, the Attorney General could order attorney-client monitoring based on "reasonable suspicion ...to believe that a particular inmate may use communications with attorneys or their agents to facilitate acts of terrorism."[119] Prior notice is required unless there has been court authorization.[120] There is no provision for judicial review, although the inmate may seek administrative review. The regulations also provide for a "privilege team," not involved in the underlying investigation,[121] although the specific tasks of the privilege team are not spelled out.[122]

In *Al Odah v. United States*,[123] the court ruled on whether detainees at Guantanamo were entitled to counsel to assist them in challenging their detention as authorized by the Supreme Court in *Rasul v. Bush*.[124] Apparently because of its position that the detainees were not entitled to counsel, the government advised that it would permit the detainees to consult with counsel, but that a privilege team would "monitor [and record] oral communications in real time between counsel and the detainee during any meetings" and would "review all written materials brought into or out of the meeting by counsel ...," including notes taken by the attorney during his consultations with his client.[125] These procedures were justified on a general "national security" rationale.[126] The court ruled that the detainees did have a right to counsel[127] and rejected the monitoring provisions, finding that the government's justifications for monitoring to be "thinly

---

118 28 C.F.R. § 501.3(a).
119 28 C.F.R. § 501.3(d).
120 § 501.3(d)(2).
121 § 501.3(d)(3).
122 A different, and still valid, regulation prohibits auditory monitoring of attorney-client meetings at federal prison. 28 C.F.R. § 543.13(e).
123 *Al Odah v. United States*, 346 F.Supp.2d 1 (D.C.D.C. 2004).
124 *Rasul v. Bush*, 524 U.S. 466 (2004).
125 346 F.Supp.2d at 3.
126 *Id.* at 9.
127 *Id.* at 5-8.

supported"[128] and "flimsy".[129]

The government cited C.F.R. Section 501.3 as an example of permissible monitoring but did not rely directly on the regulation as authority.[130] The court was unimpressed, noting that the propriety of that regulation had never been passed upon and that its existence alone was not sufficient "to persuade the Court that such monitoring is proper."[131]

In a separate attack on attorney-client monitoring, a group of federal defenders filed a complaint in the Eastern District of New York alleging that the policy of the Bureau of Prisons to video- and audiotape conversations with the attorneys' detained clients violated the federal wiretapping statute (Title III) and the Fourth and Fifth Amendments to the U.S. Constitution.[132] The particular detainees had been arrested on immigration charges and crimes not including terrorist crimes; they had been rounded up in the aftermath of 9/11. The recording, which occurred at least between October 2001 to February 2002, had not been authorized by the Attorney General under C.F.R. Section 501.3.[133]

The district court found that the complaint stated a claim under Title III ("... I find that the facts alleged in the complaint, if proven, would establish that [the warden] violated plaintiffs' rights under the Wiretap Act to engage in oral communications with Detainees in the Visiting Area without having those communications intentionally intercepted."[134] The court also found that the attorneys had a reasonable expectation of privacy in their conversations with the detainees because of the special status of communications between attorney and client, and in

---

128 *Id.* at 10.

129 *Id.* at 12.

130 *Id.* at 13, n. 14. We can only speculate that the government did not want to take a position inconsistent with its position in other cases that Guantanamo was outside the jurisdiction of the United States legal system.

131 *Id.* at 13.

132 *Lonegan v. Hasty*, 436 F. Supp.2d 419 (E.D.N.Y. 2006).

133 436 F. Supp.2d at 424.

134 436 F. Supp.2d at 430.

spite of the fact that the conversations took place in a prison with video cameras in the area.[135]

At about the same time, the Department of Justice applied to the District Court for the District of Columbia for permission to review 1,100 pounds of confiscated personal papers taken from prisoners in Guantanamo Bay as part of an investigation into recent suicides that, the government claimed, had been furthered by the inmates' misuse of attorney-client documents. The government proposed that a "filter team" would segregate potentially privileged material and present that to the court and defense counsel only, except material posing a threat to national security.[136] The court approved the government's proposal, finding that the attorney-client privilege protects "only those disclosures necessary to obtain informed legal advice which might not have been made absent the privilege,"[137] that the proposed procedures "are reasonably related to the legitimate penological interest in investigating the detainee suicides and thwarting further prison disruption,"[138] that the filter teams were the most practical way of implementing the government's legitimate policy,[139] and that any possible chilling effect "cannot be allowed ... to trump the government's investigative requirements in this sensitive situation."[140]

Similarly, in ruling on the procedures to be followed in connection with the application of Guantanamo detainees for review of their "enemy combatant" designation, the District of Columbia Circuit Court approved a government proposal for a "privilege team" to open all legal mail and search it for "prohibited content." Although the court agreed that full communication between attorney and client would help counsel present his client's defense and would aid the process of review, "[r]egrettably, however, we cannot disagree with the Government that past

---

135 *Id.* at 434-35. The court dismissed the Fifth Amendment claim, based on substantive due process, finding that such a claim was not available when the conduct complained of violated another, explicit provision, here the Fourth Amendment. 436 F.Supp.2d at 440.

136 *Hicks v. Bush*, 452 F.Supp.2d 88, 97 (D.C.D.C. 2006).

137 452 F.Supp.2d at 100 (internal citation and quotation marks omitted).

138 *Id.* at 102.

139 *Id.* at 103.

140 *Id.* at 103.

breaches of the Status Quo Order by some counsel for detainees justify the Government's proposal ... to hold all counsel accountable by screening the legal mail they send to their detainee clients."[141]

In May 2007, the Center for Constitutional Rights, on behalf of attorneys representing detainees at Guantanamo, filed a freedom of information lawsuit in the Southern District of New York seeking, among other things, information concerning whether the government was listening in on attorney-client conversations.[142] A decision on June 25, 2008, granted the government's partial motion for summary judgment on the request for records concerning warrantless electronic surveillance or physical searches "regarding, referencing or concerning" any of the attorneys.[143] The district court accepted the government's explanation that acknowledging whether the information existed or didn't "would reveal the NSA's organization, functions, and activities," information protected by the National Security Agency Act of 1969.[144] On July 31, 2008, the district court entered partial summary judgment, enabling an immediate appeal of this part of the lawsuit.[145] The appeal is still pending as of the date of this Report.[146]

E. Preliminary Conclusions Regarding Criminal Justice, the Internet, and Privacy

The expectation of privacy of one who becomes embroiled in the criminal justice system is necessarily diminished: the police may search a suspect incident to an arrest based on probable cause or pursuant to an arrest warrant; the police may search private premises based on

---

141 *Bismullah v. Gates*, 501 F.3d 178, 189 (D.C. Cir. 2007). This holding was only a small part of the decision. Subsequently, on the government's petition for certiorari, the U.S. Supreme Court vacated the judgment and remanded for further proceedings in light of *Boumediene v. Bush*, U.S. 128 S.Ct. 2229 (2008), which held that detainees have the right to challenge by means or a writ of habeas corpus the basis for their confinement.

142 Wilner v. Nat'l Security Agency, 07-CV-3883 (DLC).

143 *Wilner v. National Security Agency*, 2008 WL 2567765 (S.D.N.Y., 6/25/2008).

144 50 U.S.C. § 402. 2008 WL 2567765 at *4. *See* Center for Constitutional Rights, "Judge Rules Government Can Keep Secret Whether It Spied on Guantanamo Attorneys," http://ccrjustice.org/newsroom/press-releases/judge-rules-government ....

145 2008 WL 2949325 (S.D.N.Y. 7/31/2008).

146 The *Wilner* plaintiffs filed their appellate brief on December 12, 2008. Related legal documents are available at http://ccrjustice.org/ourcases/current-cases/wilneer-v.-national-security-agency).

a search warrant; written and oral communications between an individual placed in detention following an arrest and family or friends will be monitored; and jail cells are subject to searches for contraband. A conviction results in more infringements on privacy interests. Even the person placed on probation is subject to search by the probation officer, as is that person's home and possibly place of business. Sex offenders may be required to register on a publicly available registry.

These limits on privacy are by and large appropriate and justified by the special circumstances. However, sometimes the balance is not struck appropriately. The Second Circuit has struck down the blanket policy of some Police or Corrections Departments to strip search all misdemeanant arrestees, finding that the invasion of privacy was unjustified without particularized suspicion that the arrestee is concealing contraband.[147]

Sometimes the publicity of an arrest causes an invasion of privacy that outweighs a governmental interest. For the purpose of deterring potential drunk drivers, the Nassau County Executive posted on its web site the name, picture and identifying information of persons arrested for driving while intoxicated and included such information in press releases. In *Bursac v. Suozzi*,[148] the court found that the petitioner had established the "stigma plus" elements of a due process claim and directed the County Executive to remove the petitioner's arrest record from the web site.[149]

---

147 *Hartline v. Gallo*, 546 F.3d 95, 97 (2d Cir. 2008) (Southampton Police Department); *Ciraolo v. City of New York*, 216 F.3d 236 (2d Cir. 2000) (New York City Department of Correction) (affirming the jury's award of compensatory damages and reversing only the award of punitive damages); s*ee also In re County of Erie*, 546 F.3d 222 (2d Cir. 2008) (ongoing litigation concerning strip search policies at the Eric County Jail); *Marriott v. County of Montgomery*, 2005 WL 3117194 (2d Cir., dec. 11/22/2005) (n.o.r.) (affirming preliminary injunction enjoining automatic strip searches for misdemeanants at Montgomery County jail).

148 *Bursac v. Suozzi*, 2008 WL 4830541, 2008 N.Y. Slip Op. 28437 (Sup. Ct. Nassau Co., dec. 10/21/2008).

149 *Id.* at *6, *10, *See also* "Driver Sues County, Newspaper Over 'Shame' Gallery," New York Law Journal, September 15, 2008, News in Brief, p. 1; "Lawyer Sues County Over Internet 'Wall of

By contrast, in a related case, the Court of Appeals held that the Constitution did not prohibit the state from maintaining a registry of suspected child abusers so that the information could be made available to social workers investigating possible child abuse, potential employers and licensing agencies in the child care field. However, the Court ruled that a proper balance of the interests of the State in cutting down on the opportunities for child abuse and the interests of the individuals who might be erroneously included in the register required that the information not be disseminated until the report of abuse had been substantiated by a fair preponderance of the evidence.[150]

There are many other examples of the damage done by the easy availability of private information on the Internet. One prominent example is reporting done by agencies that specialize in background checks for third parties. For example, the controversial private intelligence agency, ChoicePoint, that proclaims itself "the premier provider of decision-making insight to businesses and government,"[151] has been the subject of several recent lawsuits due to its irresponsible dissemination of private information.

In *Pendergrass v. ChoicePoint*,[152] a Rite Aid store in Philadelphia terminated Mr. Pendergrass as shift supervisor and sent ChoicePoint a report of "Cash Register Fraud and Theft of Merchandise." Although no criminal charges were ever filed and Pendergrass was vindicated at an unemployment compensation hearing, CVS, Walgreens and Target denied him employment

---

Shame,'" New York Law Journal, October 8, 2008, News in Brief, p. 1. In *People v. Letterlough*, 86 N.Y.2d 259 (1995), the sentencing judge had imposed as a condition of probation the requirement that a convicted drunk driver affix to his license plate a fluorescent sign stating "convicted dwi." The Court of Appeals found that the condition did not further the goal of probation (that is to advance rehabilitation) but was intended to warn the public of a threat. Without specific legislative authorization, the condition was illegal.

150 *Matter of TT. v. Dowling*, 87 N.Y.2d 699, 703 (1996).

151 *See* http://www.choicepoint.com/about/overview.html, ChoicePoint's Official Web Site.

152 *Pendergrass v. ChoicePoint, Inc.*, 2008 WL 5188782 (E.D.Pa., dec. 12/10/2008).

because (according to his lawsuit) of the information supplied by ChoicePoint.[153] The district court found his lawsuit for defamation could continue, rejecting a statute of limitations defense.[154] The Court distinguished the "single publication" rationale aimed at preventing an indefinite statute of limitations where publication was made in a newspaper or magazine and a publication made by a report "not made available to the public but only to subscribing members of a database."[155]

In *Ewbank v. ChoicePoint,*[156] Fieldglass, Inc. offered a job to Anne Ewbank as a sales representative contingent on a background check. ChoicePoint inaccurately reported a conviction for possession of a controlled substance. Ewbank had been charged with that offense, but in fact had been dismissed. Nevertheless, Fieldglass withdrew its offer after giving Ewbank only one week to show the report was incorrect. Although ChoicePoint eventually gave the employer the corrected information at Ewbank's request, the damage had already been done. Ewbank lost her Fair Credit Reporting Act ("FCRA") claim when the court ruled that ChoicePoint had not exhibited "malice or willful intent" and eventually deleted the inaccurate information.

While ChoicePoint currently claims to "strongly promote[s] the responsible use of information as a fundamental plank of its business model, including strict standards regarding the use and dissemination of personal information,"[157] its legal history includes a $15 million payment in 2006 to settle a lawsuit with the FTC. [158] The complaint, filed in the U.S. District

---

153 *See* Chad Terhune, "The Trouble with Background Checks: Employee screening has become big business, but not always an accurate one." BusinessWeek May 29, 2008. http://www.businessweek.com/magazine/content/08_23/b4087054129334.htm?campaign_id=rss_smlbz.

154 *Id.*

155 2008 WL 5188782 at *4.

156 *Pendergrass v. ChoicePoint, Inc.*, 551 F. Supp.2d 563 (N.D. Texas 2008).

157 *See* http://www.ChoicePoint.com/about/overview.html.

158 *See* Stipulated Final Order and Judgment and Order for Civil Penalties, Permanent Injunction, and

Court for the Northern District of Georgia, alleged that the personal information of 163,000 consumers had been compromised, including nearly 10,000 credit reports, resulting in at least 800 cases of identity theft.[159] During the well-publicized criminal prosecution was of Olatunji Oluwatosin for identity theft, ChoicePoint revealed that more than 50 of the clients to whom they gave consumers' personal information appeared to be phony businesses.[160]

The misuse of personal information raises serious questions concerning whether the growing circulation of such information strikes the proper balance between privacy rights and the public interest. Criminal records are useful for purposes of law enforcement and may help employers avoid negligent hiring claims for example. On the other hand, they result in crippling – and unfair – prejudice that can be counterproductive to rehabilitative goals. Employment is undoubtedly associated with reduced recidivism, yet employers are increasingly discriminating because of the new availability of personal information via the Internet and computer databases. For another example, financial information is useful for banks and businesses to make credit and lending decisions, but the mass availability of private financial information has lead to dissemination of this information into the wrong hands, facilitating identity theft.

One of the arguments made by the County in *Bursac v. Suozzi* was that the posted information about the drunk driving arrest was a matter of public record. The court noted that when a public record is placed on the Internet, technology makes the information easy to locate throughout the world and also creates a permanent record regardless of the eventual outcome of

---

Other Equitable Relief, in *U.S. v. ChoicePoint, Inc.*, Civil Action No. 1 06-CV-0198, filed February 15, 2006, available at: http://www.ftc.gov/os/caselist/ChoicePoint/stipfinaljudgement.pdf.

159 *See* FTC's Complaint in *U.S. v. ChoicePoint Inc.*, 1-06-CV-0198, filed January 30, 2006, http://www.ftc.gov/os/caselist/ChoicePoint/0523069complaint.pdf.

160 *See* Robert O'Harrow, Jr., "ChoicePoint Data Cache Became a Powder Keg: Identity Thief's Ability To Get Information Puts Heat on Firm." Washington Post, March 5, 2005, 2008. http://www.washingtonpost.com/wp-dyn/articles/A8587-2005Mar4.html.

the underlying matter.[161] As the court said:

> It is the scope and permanency of public disclosure on the Internet by a governmental agency that distinguishes the County's "Wall of Shame" from traditional and regular forms of reporting and publication such as print media.[162]

As is evident from this Report, the very existence of the Internet has changed things and requires a renewed vigilance to ensure that the vastly increased potential for exposure is appropriately controlled to ensure that privacy rights are infringed only for the best of reasons.

III. FEDERAL AND STATE LAWS AFFECTING THE PRIVACY OF HEALTH INFORMATION

A. HIPAA Privacy and Security Regulations

"HIPAA" is a shorthand term for the Health Insurance Portability and Accountability Act of 1996.[163] HIPAA was enacted to address a broad range of reform issues in the healthcare market,[164] not the least of which was the privacy and security of patient medical information.[165] The goal of the privacy component of HIPAA was to establish an appropriate minimum standard of protection for patient medical information in all formats. The goal of the security component of HIPAA was to establish an appropriate minimum standard of protection for patient medical information in electronic formats. Whether HIPAA achieved either of those goals has been the subject of some debate.[166]

More recently, the American Recovery and Reinvestment Act of 2009[167] ("ARRA") expanded HIPAA's application and, among other changes, significantly increased the penalties for HIPAA violations. The legislation intended to correct what was largely perceived as one of

---

161 2008 WL 4830541 at *8-9.

162 *Id.* at *9.

163 Pub. L. No. 104-191, 110 Stat. 1936 (1996).

164 HIPAA also included group and individual insurance market reforms, fraud and abuse controls, and tax reforms for medical savings accounts and long term care insurance.

165 For the parade of horribles, *see* 65 Fed. Reg. 82467 (Dec. 28, 2000).

166 *See* Deane Waldman, "Shoot HIPAA the Hippo," posted at The Huffington Post, June 30, 2008.

167 Pub. L. No. 111-5, ____ Stat. ____ (2009).

HIPAA's shortcomings: the lack of meaningful enforcement activity. HIPAA is the most comprehensive and significant body of medical privacy standards in effect today.

Regulations under HIPAA are segmented into three distinct but interrelated parts: (i) privacy standards; (ii) security standards; and (iii) transactional standards. The transactional standards[168] are not particularly relevant from either a privacy or security perspective, but rather provide a standard framework for common healthcare transactions such as checking eligibility, billing, and remitting payments. The security standards,[169] while focused more on technical matters, both supplement and augment the privacy protections available under the privacy standards. The privacy standards[170] are intended to provide cradle-to-grave (and beyond) guidance for the handling of health information.

1. Privacy Standards

The fundamental information regulated by the HIPAA privacy standards is "protected health information,"[171] or "PHI," and the fundamental entities regulated by HIPAA are "covered entities."[172] Physicians, hospitals, and health insurers are "covered entities." Entities such as newspapers, police agencies, professional baseball teams, and schools (with rare exception) are not.

HIPAA focuses on two basic activities that can occur with PHI: use and disclosure. Use is any given use – such as analysis, examination, or application – of PHI within the covered entity.[173] Disclosure is the release, transfer, or transmission of PHI, by whatever means, to a

168 45 C.F.R. Part 162 – Administrative Requirements.
169 45 C.F.R. Part 164, Subpart C – Security Standards for the Protection of Electronic Protected Health Information.
170 45 C.F.R. Part 164, Subpart E – Privacy of Individually Identifiable Health Information.
171 45 C.F.R. § 160.103.
172 *Id*.
173 *Id*.

party outside of the covered entity.[174] The privacy standards describe the permitted uses and disclosures of PHI in detail.

HIPAA is a proscriptive regulation: it prohibits all uses or disclosures of PHI except those that take place as described in, and in accordance with, the privacy standards. There are two basic documents that facilitate uses and disclosures of PHI. One is the "notice of privacy practices"; the other is the "authorization."

The notice of privacy practices, or "NPP," is made available by the covered entity and is intended to provide notice to individuals of how the covered entity uses and discloses PHI in its possession. In theory, a notice of privacy practices is supposed to describe the particular uses and disclosures a covered entity may undertake with PHI in sufficient detail to put the patient on notice of such uses.[175] In practice, notices of privacy practices have become a sort of generalized statement of HIPAA's default use and disclosure rules.

With a functional NPP in place, covered entities may use PHI, and in some cases disclose PHI, for three basic functions: (1) treatment; (2) payment; (3) and healthcare operations. Within this paradigm, a physician can, for example, see a patient's hospital records when the physician is treating the patient (treatment); the physician can send records to a health insurer to support a claim for payment (payment); and the physician can make patient records available to a quality assurance reviewer (healthcare operations), all based on the terms of the NPP and without a specific authorization from the patient.[176]

"Healthcare operations" is perhaps the broadest of the three functions. Its definition includes specific examples of activities such as conducting quality assessment and improvement, conducting peer review, engaging in underwriting and premium rating, and conducting

---

174 *Id.*

175 45 C.F.R. § 164.520.

176 45 C.F.R. § 164.502.

credentialing and recredentialing of health care providers. Interspersed among these specific examples are vague catchall phrases, such as "related functions," and generalized categories such as "business management and general administrative activities."

Beyond disclosures for these general purposes of treatment, payment and healthcare operations, covered entities may use or disclose PHI for twelve different purposes specifically identified in the regulation.[177] These purposes include: disclosures in connection with judicial proceedings; law enforcement investigations; state oversight (such as an Office of Professional Medical Conduct ["OPMC"] investigation), and more exotic purposes such as national security and intelligence activities. HIPAA includes an additional, smaller listing of uses and disclosures to which the individual must be given an opportunity to agree or object, such as for hospital directories, or for disaster recovery purposes.[178]

If a covered entity wishes to use or disclose PHI for any reason other than treatment, payment, or healthcare operations, or for a specific purpose identified in the standards, the covered entity must obtain an authorization from the patient. The authorization must meet specific criteria outlined in HIPAA regulations, including (among other criteria) an expiration date, a specific stated purpose for the use or disclosure, and an acknowledgment of the patient's right to revoke the authorization.[179] One example of an authorization arises when a patient sues to recover personal injury damages. To facilitate an evaluation of the plaintiff's injuries by defense counsel, the plaintiff must provide a HIPAA-compliant authorization permitting the plaintiff's physician to disclose medical records to the defendant's attorney.[180]

Covered entities may use business associates in connection with any permitted use or

---

177 45 C.F.R. § 164.512.

178 45 C.F.R. § 164.510.

179 45 C.F.R. § 164.508.

180 For a fuller discussion of this scenario, see *infra* Section III.C. Disclosure of Medical Records and Health Information in Litigation.

disclosure of PHI. The business associate must have a business associate contract with the covered entity that meets specific criteria outlined in the regulations.[181] The contract must, for example: (i) describe the permitted and required uses of PHI by the business associate; (ii) prohibit the business associate from using or disclosing PHI in a manner other than as provided in the contract; (iii) require the business associate to use appropriate safeguards to prevent impermissible uses or disclosures of PHI; and (iv) return or destroy PHI in its possession once the business associate relationships have concluded.[182] The criteria provided here are exemplary only and are not exhaustive.

Prior to the HIPAA amendments in ARRA, business associates were obligated primarily only by these contracts with covered entities. The ARRA amendments, however, make it a HIPAA violation for a business associate to use or disclose PHI other than as provided in the business associate contract,[183] effectively subjecting business associates to direct regulation by overseeing agencies. Additionally, business associates will be subject to periodic audits under ARRA to ensure compliance.[184]

Lawyers performing legal services for a covered entity – such as a physician's business attorney, or outside counsel to a health plan – can be business associates of the covered entity if, in the performance of their work, the lawyer will create, receive, or have access to PHI on behalf of the covered entity. The direct regulation and audit of business associates under the ARRA amendments raise interesting questions about the future interplay of HIPAA and attorney-client privilege.

---

181 45 C.F.R. § 164.504(e).

182 45 C.F.R. § 164.403(e)(2). The Federal Office of Civil Rights, which oversees the HIPAA privacy standards, has developed a "model business associate contract" that can be useful for comparative purposes. Accessible as of this writing at www.hhs.gov/ocr/hipaa/contractprov.html and on file with the authors.

183 ARRA § 13404.

184 ARRA § 13411.

The existence of a business associate contract does not obviate the need for patient authorization. If the use or disclosure to the business associate is for payment purposes, for example, the covered entity need not obtain a patient authorization because such disclosures are permitted without one. But if the use or disclosure requires an authorization, one must be obtained in addition to having the business associate contract in place.

In general, uses and disclosures of PHI are subject to the "minimum necessary" rule, which means that only the minimum amount of information necessary to accomplish the purpose may be used or disclosed.[185] For example, if it is not necessary for patient names and phone numbers to be included on records used internally for peer review purposes (which is a "healthcare operation"), then patient names should be excised from records copied and circulated for such purposes. The minimum necessary rule does not apply to disclosure for treatment purposes, disclosures to the individual, or disclosures pursuant to an authorization – among others.[186] The ARRA amendments promise, by August 2010, new and comprehensive guidance on what constitutes "minimum necessary."[187]

HIPAA is intended to ensure that individuals are provided timely access to records containing their PHI.[188] It also permits individuals to amend their records (or in some cases, annotate them),[189] and to discover what disclosures of their PHI have been made. The latter is referred to as the "accounting" standard because it requires covered entities to render an accounting of PHI disclosures. Until recently, only uses or disclosures other than treatment, payment, healthcare operations, and national security (among a few other exclusions) needed to

185 45 C.F.R. § 164.502(b).
186 45 C.F.R. § 164.502(b)(2).
187 ARRA § 13405(b).
188 45 C.F.R. § 164.524.
189 45 C.F.R. § 164.526.

be accounted for.[190] Under the ARRA amendments, however, covered entities making certain uses of electronic health records must maintain information about accesses and disclosures made using the software.[191] This provision will result in an increase both in the number of requests for accountings as well as in the number of responsive accountings covered entities will need to produce.

Covered entities under HIPAA privacy standards are subject to extensive documentation requirements, including maintenance of current policies and procedures implementing HIPAA and documentation of compliance.[192] Covered entities must also make specific personnel designations, and engage in specified training activities. Records demonstrating compliance with the privacy standards must be kept for a minimum of six years.

Under the ARRA amendments, covered entities may not "directly or indirectly receive remuneration in exchange for any protected health information of an individual" unless a valid authorization is in place.[193] The law includes a number of exceptions to this rule, such as public health activities, research, treatment, and mergers and acquisitions, among several others. This language and the accompanying list of exceptions should look familiar to health lawyers accustomed to Stark Anti-referral/Anti-Kickback Statute analyses, and will likely create an analogous set of headaches for lawyers constructing business relationships involving covered entities or their business associates.

2. Security Standards

HIPAA security standards supplement and support the privacy standards, and generally address the physical, technical, and administrative safeguards covered entities must put in place

190 45 C.F.R. § 164.528.
191 ARRA § 13405(c).
192 45 C.F.R. § 164.530.
193 ARRA 13405(d).

to protect electronic PHI (or, "ePHI").[194] Physical safeguards[195] include, for example, securing network computers housing ePHI behind locked doors, and then controlling access to those computers. Technical safeguards[196] include the use of passwords to authenticate individuals using computers housing ePHI, using "role-based access" to delineate what users may see and not see when using computers housing ePHI, and the maintenance of "audit trails" as a record of which users have accessed ePHI and what they have done with it. Administrative safeguards[197] include policies and procedures for defining and granting access rights, and for securing ePHI when employees terminate their employment.

Prior to the enactment of ARRA, security standards were directly applicable only to covered entities. Business associates were required through their contracts to implement reasonable physical, technical, and administrative safeguards to protect ePHI but were answerable only to the covered entity. ARRA applies HIPAA security provisions directly to business associates.[198] This will require business associates to take a new and deeper look at their security practices.

Security standards are either "required" or "addressable." Required standards must be implemented. Addressable standards must be considered, and, if feasible for the organization, must be implemented. One example of an addressable standard is PHI encryption.[199] When the security standards were first promulgated, many organizations examined encryption and determined that it was too expensive or would compromise performance too much to justify the protections. Under the circumstances at the time, it was not feasible for the organization to

194 45 C.F.R. § 164.306.
195 45 C.F.R. § 164.310.
196 45 C.F.R. § 164.312.
197 45 C.F.R. § 164.308.
198 ARRA § 13401(a).
199 45 C.F.R. § 164.312(e)(2)(ii).

implement the standard. Since then, the protections provided by encryption have increased, while the cost of encryption and its effect on performance have both decreased. As a result, some organizations are now revisiting the feasibility of encryption and are deploying it in areas where the protections justify the cost.

The security standards do not mandate specific technologies. Covered entities may select the best strategy available to meet the standard. In the case of each standard, the covered entity must review the options available, and select the one that best accomplishes the standard in light of the covered entity's own risk analysis and cost benefit analysis.[200] As under the privacy standards, covered entities under the security standards must make certain personnel designations, engage in specific training activities, and maintain documentation of their compliance.[201]

The ARRA amendments create a new requirement that covered entities notify affected individuals in the event of a "breach," which is defined as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information."[202]

The principal remedy when PHI is misused under the HIPAA privacy or security standards is to file a complaint with the U.S. Department of Health & Human Services, Office of Civil Rights ("OCR").[203] A complaint may be tendered by any individual, and need not be the individual who is the subject of the information. The complaint may be made a number of ways, but the easiest way is to submit a complaint through the OCR web site.[204] Individuals may also complain to the covered entity using the procedure identified in the NPP. There is a limitation of

---

200 45 C.F.R. § 164.306(b).
201 45 C.F.R. §§ 164.314, 164.316.
202 "Breach" is defined at ARRA § 13400 (1); for the notice obligations, see ARRA § 13402(a).
203 5 C.F.R. § 164.306(a).
204 www.hhs.gov/ocr/hipaa.

180 days to make the complaint, measured from when the complainant "knew or should have known that the act or omission occurred."[205] Although the regulation does not provide for an extension of this period, an OCR fact sheet indicates OCR may extend the 180-day period for "good cause."[206]

Prior to the ARRA amendments, covered entities violating HIPAA were subject to civil monetary penalties of up to $100 per day per violation to a maximum of $25,000 per year for identical violations. The ARRA amendments create a tiered penalty structure, with unintentional violations subject to a minimum fine of $100 per day up to $25,000 per year, and violations due to "willful neglect" subject to potential fines of at least $50,000 per violation up to $1.5 million per year.[207] Several other tiers of penalties exist in between. The enhanced penalties took effect February 17, 2009---the date ARRA was signed.

In addition to the enhanced penalties, the new law permits State attorneys general to bring a civil action in U.S. District Court in any case in which the attorney general "has reason to believe that an interest of one or more of the residents of that State has been or is threatened or adversely affected by any person who violates a provision of [HIPAA]."[208] Damages in actions brought by the attorneys general are limited to $100 per violation to a maximum of $25,000 per year. The law also contemplates that, by February 2012, regulations will have been promulgated granting individuals harmed by a HIPAA violation the right to receive a percentage of any civil monetary penalty collected with respect to the offense.[209]

The final version of HIPAA privacy standards became effective October 15, 2002, with

---

205 45 C.F.R. § 164.306(b)(3).

206 Fact Sheet, U.S. Dept. of Health & Human Services, Office for Civil Rights, "How to File a Health Information Privacy Complaint with the Office of Civil Rights," (Aug. 2008). Available as of this writing at www.hhs.gov/ocr/privacyhowtofile.pdf and on file with the authors.

207 ARRA §13410.

208 ARRA § 13410(e).

209 ARRA § 13410(c).

compliance required by April 14, 2003. HIPAA security standards became effective April 21, 2003, with compliance required by April 20, 2005. On both privacy and security, it is estimated that compliance was initially around 70% for payors and providers, improving to about 80% at the end of the first year.[210] By 2006 compliance had improved only marginally from the 2004 results, suggesting a core of recalcitrant covered entities that cannot or will not implement either the privacy or security standards.[211] It remains to be seen whether the enhanced penalties described above and the increased enforcement trend discussed in Section III.F., Infra, will eventually address this remaining pocket of non-compliance.

B. New York State Laws Regarding Health Information Privacy

New York does not have a comprehensive statute or regulation like HIPAA to address the privacy and security of patient health information. Rather, the state has a patchwork of laws and regulations that: (i) impose obligations on specific classes of providers, such as physicians, hospitals, nursing homes and mental health programs; (ii) set forth enhanced protections for specific types of health information, *e.g.*, HIV information and genetic information; (iii) provide patients and their representatives a right to access their own information; and (iv) address disclosure of medical records and information in the context of litigation.

Before summarizing key provisions of New York privacy laws and regulations, it must be noted that HIPAA's preemption provision significantly impacts New York's laws on the privacy and security of health information, overriding some and leaving others intact. The HIPAA preemption provision generally provides that a HIPAA standard will preempt a contrary state law relating to privacy of health information unless the state law is "more stringent" than the

---

210 Grove, Tom, "Countdown to Compliance for HIPAA: Results of the Winter 2004 Healthcare Industry HIPAA Compliance Survey," Phoenix Health Systems, Inc., 2004. Available as of this writing at: www.ehcca.com/presentations/HIPAA8/grove.ppt and on file with the author.

211 U.S. Healthcare Industry HIPAA Compliance Survey Results: Summer 2006, Phoenix Health Systems, Inc., 2006. Available as of this writing at www.himss.org/content/files/SummerSurvey2006.pdf and on file with the author.

HIPAA standard. "More stringent" means that the state law is more restrictive as to a use or disclosure, or more expansive as to the rights of individuals to access or amend their own information.

In some respects, New York's requirements are less strict than HIPAA requirements. For example, New York does not specify the form or contents of a patient's consent for the release of protected health information by a healthcare provider, whereas HIPAA authorization requirements are quite detailed. But in other respects, New York law is more stringent than HIPAA principles. For instance, HIPAA allows a covered entity to disclose protected health information to another provider for treatment purposes, or to a payor for payment purposes, without the patient's consent, whereas New York requires a patient's consent for such disclosures.

The principal New York statutes and regulations governing the privacy of health information are summarized below. Provisions of state law that are preempted by HIPAA are noted in the course of that summary, and further HIPAA preemption information is charted below.

C. NYS Laws and Regulations Governing Specific Types of Providers

1. Physicians and Other Professionals

The State Education Law and Board of Regents regulations provide that it is professional misconduct for a physician, physician's assistant ("PA") or specialists' assistant ("SA") to reveal "personally identifiable facts, data, or information obtained in a professional capacity without the prior consent of the patient, except as authorized or required by law."[212] In general, a violation would be addressed by an action by the OPMC to sanction the physician, PA or SA.

The Board of Regents regulations governing other professionals provide that it is

[212] NY Education Law § 6530(23).

"unprofessional conduct" to disclose "personally identifiable facts, data, or information obtained in a professional capacity without the prior consent of the patient, except as authorized or required by law."[213] Accordingly, a nurse, social worker, physical therapist, psychologist or other professional would be subject to professional discipline by the Board of Regents for such conduct.

2. Hospitals

New York State Department of Health ("DOH") regulations governing hospitals impose significant privacy and security standards relating to medical records, patient rights, and medical staff by-laws.[214] With respect to medical records, a hospital must ensure the confidentiality of patient records and release records or information from records "only to hospital staff involved in treating the patient and individuals as permitted by Federal and State laws." This provision has been interpreted to require hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes.[215] A hospital must also institute safeguards to protect the security of medical records, including a system "to ensure the integrity of the authentication and protect the security of all transmissions, records and record entries" as well as implement policies to ensure the security of electronic or computer equipment from unwarranted access.

3. Nursing Homes

The Public Health Law ("PHL") and DOH regulations set forth certain rights of nursing home residents, including the right to "confidentiality in the treatment of personal and medical records."[216] In addition, DOH regulations require nursing homes to "keep confidential all

213 8 NYCRR § 29.
214 10 NYCRR § 405.10.
215 *See* Williams v. Roosevelt Hospital, 66 N.Y.2d 391(1985).
216 NY PHL § 2803-c.3(f); 10 NYCRR § 415.3(d).

information contained in the resident's records, regardless of the form or storage method of the records, except when release is required by: (1) transfer to another healthcare institution; (2) law; or (3) the resident."[217]

4. Home Care

All categories of home healthcare patients have the right to "privacy, including confidential treatment of medical records, and refusal of their release to any individual outside of the agency except in the case of the patient's transfer to a healthcare facility, or as required by law or third party payment contract."[218] DOH regulations also require all categories of home healthcare providers to maintain "a confidential clinical record for each patient, and provide that such records must be "kept securely."[219]

5. Mental Health and Mental Retardation Providers

NYS Mental Hygiene Law Section 33.13 governs the confidentiality of records maintained by facilities licensed or operated by the New York State Office of Mental Health ("OMH") and Office of Mental Retardation and Developmental Disabilities ("OMRDD"). As a result, the provision does not apply to all patient mental health or mental retardation information. For instance, such laws would not apply to mental health treatment records created by psychiatrists, psychologists, primary care physicians or other professionals outside of an OMH licensed or operated mental health facility; nor would it apply to a hospital's general emergency department records of visits for mental health services. However, these laws do apply to records created by mental health programs, including OMH-licensed hospital mental health units.

The relationship between NYS Mental Hygiene Law ("MHL") Section 33.13 and HIPAA

---

[217] 10 NYCRR § 415.22(2).
[218] 10 NYCRR §§ 763.2((a)(1), 767.1.
[219] 10 NYCRR §§ 763.6(c), 767.6(b).

is complex, and OMH has issued a comprehensive analysis.[220] At the risk of oversimplifying, it is generally safe to assume that the confidentiality standards set forth in Section 33.13 are either consistent with or more stringent than HIPAA, and thus should be followed.

Broadly stated, MHL Section 33.13 provides that information maintained by such facilities or programs, including the identification of patients or clients, clinical records or clinical information tending to identify patients or clients are confidential and cannot be released to any person unless one of a list of exceptions applies. The exceptions include a release of such information with the consent of the patient or of someone authorized to act on the patient's behalf, but only to persons and entities "who have a demonstrable need for such information."

Another key exception is that mental health information can be released pursuant to court order, however, the court order must require disclosure "upon a finding by the court that the interests of justice significantly outweigh the need for confidentiality..." Accordingly, practitioners should note that it is not sufficient to just secure a court-ordered subpoena and expect a mental health provider to furnish records. Rather, the order must set forth the required finding by the judge.

Information can also be released to a "qualified person" under MHL Section 33.16. The referenced section MHL Section 33.16 is discussed further below under the section on the right of access to medical information.

MHL Section 33.13 also includes the state's so-called "Tarasoff" exception,[221] which allows disclosures for warning purposes. The disclosure is permitted when a treating psychiatrist or psychologist has determined that a patient or client presents a serious and imminent danger to

---

220 OMH HIPAA Preemption Analysis, *available at* http://www.omh.state.ny.us/omhweb/hipaa/preemption_html.

221 *See Tarasoff v. Regents of the University of California*, 17 Cal. 3d 425, 551 P.2d 334, 131 Cal. Rptr. 14 (Cal. 1976) (mental health professionals have a duty to protect individuals who are being threatened with bodily harm by a patient**).**

that individual. Significantly, the provision states that it should not "be construed to impose an obligation upon a treating psychiatrist or psychologist to release information."

Another relatively recent exception, intended to facilitate local coordination of care with each other, allows hospital emergency rooms and mental health programs to share mental health information about a patient.[222]

6. Alcoholism and Substance Abuse Providers

Regulations of the NYS Office of Alcoholism and Substance Abuse Services ("OASAS") require facilities and programs licensed or funded by that agency to comply with federal regulatory standards regarding the confidentiality of alcohol and drug abuse patient records.[223]

Federally assisted alcohol and substance abuse providers are also subject to those federal regulations. Those federal regulations[224] are quite strict and detailed, and generally: (i) provide that covered programs, and certain recipients of information from covered programs, are prohibited from using or disclosure and use of alcohol and drug abuse patient records except in specific circumstances; (ii) specify various exceptions, such as disclosures with consent by or on behalf of the patient, communications within a program among personnel providing treatment to the subject, communications to law enforcement personnel regarding a crime on the premises, and reporting child abuse or neglect; (iii) prescribe who may consent on behalf of an incompetent, deceased or minor patient; (iv) specify nine elements that must be in a consent for it to be valid; (v) require notice to patients of confidentiality requirements; and (vi) set forth basic security standards, *e.g.*, that written records must be "maintained in a secure room, locked

---

222 MHL § 33.13(d).

223 *E.g.*, 14 NYCRR §§ 822.5, 1020.10; 1034.9, 1045.2(k)(2). (*E.g.*, 14 NYCRR § 822.5(b), which governs outpatient chemical dependency programs, states that "Patient records maintained by the outpatient service are confidential and may only be disclosed in conformity with federal regulations governing the confidentiality of alcohol and drug abuse patients' records as set forth in 42 Code of Federal Regulations Part 2 and other applicable law."

224 42 C.F.R. Part 2, Confidentiality of alcohol and drug abuse patient records.

file cabinet, safe or other similar containers when not in use."

For violations of the use and disclosure restrictions on alcohol and substance abuse services records, OASAS may impose financial penalties beginning at $500 for the first incident and up to $5,000 for subsequent incidents.[225]

7. Other

Hospices[226] and diagnostic treatment centers[227] must maintain the confidentiality of records. In addition, pharmacies utilizing a computerized prescription management system "shall provide adequate safeguards against improper manipulation or alteration of stored records."[228] Health maintenance organizations and comprehensive health services plans are generally prohibited from disclosing any information about medical services rendered to enrollees, unless the patient waives the right of confidentiality.[229]

D. NYS Laws and Regulations Governing Specific Types of Private Health Information

1. HIV/AIDS

In 1988, the New York State Legislature enacted PHL Article 27-F, which sets forth extensive requirements relating to consent for HIV testing and the confidentiality of HIV and AIDS information.

Confidentiality provision in general.[230] The confidentiality provision, in sum, provides that persons who obtain confidential HIV-related information in the course of providing any health or social service or pursuant to a release of confidential HIV-related information may not disclose or be compelled to disclose such information, except to specified categories of persons,

225 42 U.S.C. § 290dd-2; 45 C.F.R. Part 2.
226 10 NYCRR § 794.1(a)(10).
227 10 NYCRR § 751.7(g).
228 8 N.Y.C.R.R. § 29.7(a)(8)(i).
229 PHL § 4410(2).
230 NY PHL § 2782.1

including:

(1) the "protected individual" (or, when the protected individual lacks capacity to consent, a person authorized pursuant to law to consent to healthcare for the individual);

(2) a person to whom disclosure is authorized pursuant to a "Release of confidential HIV related information";

(3) a healthcare provider who provides healthcare to the protected individual, or maintains or processes medical records for billing or reimbursement and who meets other requirements;

(4) a healthcare provider or health facility when knowledge of the HIV related information is necessary to provide appropriate care or treatment to the protected individual, a child of the individual, a contact of the protected individual;

(5) third party payors, provided that, where necessary, an otherwise appropriate authorization for such disclosure has been secured by the provider;

(6) any person to whom disclosure is ordered by a court of competent jurisdiction (*see* "Court authorization," below); and

(7) various criminal justice officials.

Contact notification.[231] In 1998, the Legislature authorized physicians to disclose HIV information, under certain conditions, to a "contact" of the protected individual, *i.e.*, a person, including a spouse or sex partner, who may have been exposed to and placed at risk of transmission of HIV as a result of contact with the protected individual). Alternatively, the physician may notify a public health officer of the risk to the contact.

Redisclosure.[232] The statute prohibits a person to whom confidential HIV related information has been disclosed pursuant to PHL Article 27-F from further disclosing such information to another person except as authorized by the article, with certain exceptions.

Required notice.[233] Disclosures of confidential HIV related information made pursuant to PHL Article 27-F (except for disclosures to the individual and certain disclosures to contacts)

---

231 NY PHL § 2782.4.
232 NY PHL § 2782.3.
233 NY PHL § 2782.5.

must be accompanied or followed by a written notice about the prohibition on redisclosure, using required language.

Court authorization.[234] The statute prohibits courts from authorizing or ordering the disclosure of HIV information except upon an application: (i) showing a compelling need for disclosure of the information for the adjudication of a criminal or civil proceeding; (ii) showing a clear and imminent danger to an individual whose life or health may unknowingly be at significant risk as a result of contact with the individual to whom the information pertains; (iii) by a state, county or local health officer, showing a clear and imminent danger to the public health; or (iv) showing that that the applicant is lawfully entitled to the disclosure.

Violation of the prohibitions on use or disclosure of HIV/AIDS information can result in the imposition of a financial penalty of up to $5,000 per incident.[235]

2. Genetic Information

New York Civil Rights Law Section 79-l addresses both informed consent for genetic testing and the confidentiality of genetic test results. The key confidentiality provisions are that: (i) written informed consent must include the name of the person or categories of persons or organizations to whom the test results may be disclosed; (ii) any further disclosure of genetic test results to persons or organizations not named on the informed consent requires the further informed consent of the subject of the test; and (iii) notwithstanding the foregoing, a court may order further disclosure, but must first consider "the privacy interests of the individual subject of the genetic test and of close relatives of such individual, the public interest, and, in the case of medical or anthropological research, the ethical appropriateness of the research."[236]

Special penalty provisions apply to insurers misusing genetic information. Under

234 NY PHL § 2785.
235 Pub. Health L. §§ 2781, 2782.
236 NY Civ. Rights Law 79-l.4(d).

provisions of the Insurance Law, the Superintendent of Insurance may impose a fine of up to $5,000 for violations and may penalize insurers under the Unfair and Deceptive Acts and Practices elsewhere in the Insurance Law.[237]

Other states have similar genetic information protections.[238]

3. Other

Other New York State laws specifically protect the confidentiality of fetal death certificates and information,[239] reports of gonorrhea and syphilis cases,[240] and confidential information for medical and health use furnished with a certificate of live birth.[241]

E. Right to Access Medical Information Under New York Laws

1. Release of Medical Records

Public Health Law Section 17 gives a competent patient, or specified others acting for a minor or incapable patient, the right upon written request to require a physician or hospital to release and deliver, copies of medical records to any other designated physician or hospital, subject to some exceptions.[242] The physician or hospital may impose a reasonable charge as reimbursement for its expenses, with limits and exceptions. The charge for paper copies cannot exceed $0.75 per page, and a release of records under this section shall not be denied solely because of inability to pay.

---

237 Ins. L. § 2615.

238 *See also* Delaware Code Ann. Tit. 16 § 1224 (person cannot disclose or be compelled, by subpoena, or any other means, to disclose the identity of an individual on whom a genetic test has been performed or to disclose genetic information about the individual in a manner that permits identification of the individual unless necessary for a criminal or juvenile proceeding, or to protect the interests of an issuer in detecting or preventing fraud, material misrepresentation, or material non-disclosure; disclosure is necessary to determine paternity; disclosure is authorized by court order; made pursuant to DNA analysis and data bank requirements of § 4713 of Title 29, and others); N.J. Stat. Ann. § 10:5-47 (imposing similar restrictions on disclosure of genetic information); Or. Rev. Stat. § 192.539; Ga. Code Am. §§ 16-9-109 & 110.

239 10 NYCRR § 35.3.

240 10 NYCRR § 2.32.

241 10 NYCRR § 35.2(c).

242 PHL § 17.

2. Access to Patient Information

Public Health Law § 18 is the principal provision of New York law governing access by or on behalf of a patient to his or her own health records. Practitioners handling an issue relating to access under this section should carefully consult the DOH HIPAA preemption chart, since some elements of HIPAA prevail and some elements of PHL Section 18 prevail. Discussed below are the key features of PHL Section 18.

Upon written request by a "qualified person," a healthcare provider must provide an opportunity, within ten days, for such person to inspect any patient information concerning or relating to the examination or treatment of a subject in the possession of such healthcare provider. In addition, upon the written request of a qualified person, a healthcare provider must furnish to such person, within a reasonable time, a copy of any patient information requested.

"Qualified person" includes: (i) any properly identified subject (*i.e.*, the patient); (ii) an MHL Article 81 guardian, a parent or guardian of a minor; (iii) certain representatives of a patient's estate; and (iv) an attorney representing a qualified person or the subject's estate who holds a power of attorney from the qualified person or the subject's estate explicitly authorizing the holder to execute a written request for patient information under this section. "Patient information" is defined broadly, and includes a health assessment for insurance or employment purposes. Certain exclusions in the definition, such as the exclusion of personal notes of the practitioner, are preempted by the broader HIPAA provision on right of access.

The provider may impose a reasonable charge for all inspections and copies, not exceeding the costs incurred. The charge for paper copies cannot exceed $0.75 per page and a qualified person cannot be denied access solely because of inability to pay.

A provider can deny access to all or a part of the information if the provider determines that the request to review all or a part of the patient information can reasonably be expected to

cause substantial and identifiable harm to the subject or others which would outweigh the qualified person's right of access to the information, or would have a detrimental effect as defined under the statute.

In the event of a denial of access, the qualified person is entitled to notice of the denial and the basis for the denial, and the opportunity for review before by a "medical record access review committee" composed of members appointed by the Commissioner of Health.

3. Access to Mental Health Records

The Mental Hygiene Law sets forth the right of patients and clients of OMH licensed facilities and programs, and other "qualified persons" acting on their behalf, to access mental health records.[243] Modeled after PHL Section 18, MHL Section 33.16 provides a right of access, subject to important limitations, to the patient or client, a court-appointed guardian of a patient, the parent or guardian of a minor patient, and certain other individuals. The treating practitioner can deny access to a qualified person on the grounds that it "can reasonably be expected to cause substantial and identifiable harm to the patient or client or others" and provides for a review of such determination. Requests by a parent for a minor's information can also be denied on the basis of harm to the minor's relationship with the practitioner or with the parent.

4. New York – HIPAA Preemption Analysis

As previously noted, a HIPAA standard preempts a contrary state law relating to the privacy of health information unless the state law "is more stringent" than the HIPAA standard. In other words, when the rules conflict, the more stringent rule applies. "More stringent" means the rule that is either: (i) more restrictive as to a use or disclosure, or (ii) more expansive as to the rights of individuals to access or amend their own information.

Both the DOH and OMH have issued charts and other materials that compare the HIPAA

[243] MHL §§ 33.16.

and state privacy rules, identify where they conflict, and indicate the rule that prevails.[244] In many respects the laws are compatible, and subject entities can comply with both.

Some of the more significant conflicts between Public Health Law rules and HIPAA, and the prevailing rule are set forth in the chart below:

Issue	HIPAA	NY Law	Prevailing rule
Disclosures for treatment purposes	Does not require consent for such disclosures[245]	Requires consent for such disclosures	NY
Consent form for disclosures of general medical information	Imposes numerous requirements for a valid authorization	No special requirements	HIPAA
Access to billing records	Right of access includes access to billing records.	Right of access does not include access to billing records	HIPAA
Access to psychotherapy notes	Right of access excludes access to psychotherapy notes	Right of access does not exclude psychotherapy notes	NYS rule
Access to physician's personal notes	Right of access does not exclude physician's personal notes and observations.	Right of access excludes physician's personal notes and observations	HIPAA
Access to information from prior practitioner	Right of access does not exclude information re prior treatment by another practitioner	Right of access excludes information re prior treatment by another practitioner(18(1)(e)(iii))	HIPAA

The privacy provisions in Mental Hygiene Law Section 33.13 tend to be more stringent than HIPAA requirements, so in most instances, compliance with Section 33.13 is required. However, practitioners should consult the OMH chart for a clause-by-clause preemption analysis.

---

244 *See* "HIPAA Preemption Charts," NYS Department of Health *http://www.health.state.ny.us/ nysdoh/ hipaa/hipaa_preemption_charts.htm* (October 2002); OMH HIPAA Preemption Analysis," http://www.omh.state.ny.us/omhweb/hipaa/preemption_html.

245 10 NYCRR §§ 164.506(a), 164.506(c).

F. Federal and New York State Privacy and Security Enforcement Actions

Enforcement of the HIPAA privacy standards is the responsibility of the OCR. From the outset of HIPAA implementation, OCR's enforcement philosophy was one of voluntary compliance. Oversight activities were centered on complaints, with the goal of OCR's involvement being to bring the offending institution into compliance. Until July 2008, there were no published accounts of OCR imposing any fines or penalties on any covered entity, suggesting that OCR was not making full use of the enforcement remedies available to it.

On July 17, 2008, OCR announced a settlement agreement with a major hospital system in Seattle, Washington, resulting from OCR's investigation into the hospital's persistent noncompliance with certain HIPAA privacy standards.[246] The hospital system, Providence Health & Services, agreed to implement a corrective action plan and to pay a fine of $100,000. In its press release, OCR noted that "[w]hile [we] have successfully resolved over 6,700 Privacy and Security Rule cases by requiring the entities to make systemic changes to their health information privacy and security practices, this is the first time HHS has required a Resolution Agreement from a covered entity."[247]

Around the same time, various federal prosecutors began bringing charges under HIPAA's criminal provisions. The first federal prosecution under HIPAA occurred in 2004, when Richard Gibson of Seattle, Washington was prosecuted for HIPAA-related crimes and identity theft.[248] But a 2005 U.S. Department of Justice ("DOJ") memorandum defined a much smaller scope of criminal prosecution than what health attorneys originally envisioned.[249]

---

246 News Release, U.S. Department of Health & Human Services (July 17, 2008). Available as of this writing at: www.hhs.gov/news/press/2008pres/07/20080717a.html and on file with the author.

247 *Id.*

248 *U.S. v. Gibson*, 2:04-CR-0374-RSM, 2004 WL 2188280 (W.D. Wash. Aug. 19, 2004).

249 Memorandum for Alex M. Azar II General Counsel, Dept. of Health and Human Services, Timothy J. Coleman, Senior Counsel to the Deputy Attorney General, *Re:* Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6. Available as of this writing at

Following the memorandum, there were no HIPAA prosecutions until Leslie Howell of Oklahoma City was indicted in 2007 for selling over one hundred mental health patient files.[250] Howell subsequently pled guilty. In 2008, Dwight MacPherson, an employee of New York-Presbyterian Hospital/Weill Cornell Medical Center, was charged in Manhattan federal court with stealing some 50,000 patient files and selling some of them.[251] MacPherson's case, and others like it, seemed to signal a new era of HIPAA enforcement. The Wall Street Journal reported at the time that "hundreds" of similar cases were being considered by federal prosecutors around the country.[252] The ARRA amendments cement the DOJ's change in position, codifying the interpretation that individuals may be subject to HIPAA criminal sanctions in instances where the individual obtain PHI without authorization.[253]

Enforcement of the HIPAA security standards is the responsibility of the Centers for Medicare & Medicaid Services ("CMS"). In January 2008, CMS announced that it would begin on-site reviews of hospitals' compliance with security rules.[254] At that time, CMS said it intended to review ten to twenty hospitals and expected to complete the reviews by September. As of this writing, there has been no public discussion of the security reviews. In October 2008, however, the HHS Office of Inspector General ("OIG") released a report that roundly criticized

---

www.usdoj.gov/olc/hipaa_final.htm.

250 Press Release, "City Woman Pleads Guilty to HIPPA [sic] Violation for Disclosing Patient Information Used to Commit Identity Theft," U.S. Dept. of Justice, Western District of Oklahoma (May 8, 2008). Available as of this writing at oklahomacity.fbi.gov/dojpressrel/pressrel08/may08_08.htm.

251 John Eligon, "Worker Charged in Hospital File Thefts," N.Y. Times (Apr. 13, 2008). Available as of this writing at www.nytimes.com/2008/04/13/nyregion/13arraign.html.

252 *See* "Recent Medical Privacy Breaches Could Disrupt EHR Adoption Efforts," posted at iHealthBeat (Apr. 29, 2008). Available as of this writing at www.ihealthbeat.org/articles/2008/4/29/Recent-Medical-Privacy-Breaches-Could-Disrupt-EHR-Adoption-Efforts.aspx and on file with the author.

253 ARRA § 13409.

254 Nancy Ferris, "CMS to check hospitals for HIPAA security compliance," posted at Government HealthIT January 17, 2008. Available as of this writing at www.govhealthit.com/online/news/350176-1.html and on file with the author.

CMS for lax oversight of the security standards.[255] In the executive summary of the report, OIG stated that it found CMS had taken "limited actions" to ensure security compliance, had "not provided effective oversight or encouraged enforcement" of the security rule, and had "no effective mechanism" to ensure covered entities are complying with HIPAA.

The above discussion indicates a glacial but perceptible shift of enforcement philosophies from a complaint-based, compliance-goal program to one in which federal agencies take a more active role in auditing compliance and are more willing to impose monetary penalties as part of the corrective action. The ARRA amendments will continue and hasten this trend, given the enhanced penalty provision, audit rights, and enhanced criminal liability provisions included in the law.

Generally speaking, the enforcement rights to federal and state privacy laws belong to the enforcing government agencies. The 2009 ARRA amendments do include a limited grant of jurisdiction to State attorneys general to bring enforcement actions based on HIPAA violations, opening a new enforcement front at the state level. Additionally, in some cases, wrongful use or disclosure of medical information may support causes of action for breach of confidentiality, breach of privacy, and breach of fiduciary duty, including the application of punitive damages.[256]

G. Accessing and Protecting Patient Health Information

1. Accessing Patient Health Information

Access to patient health information is highly-regulated and is subject to a complex blend of often-conflicting federal and state rules. As with most privacy-related matters, attorneys should not assume that a client's permission letter, or power of attorney, or custom-drafted consent, will be sufficient to allow production of client's records; as often it will not. In

---

255 Audit A-04-07-05064, U.S. Dept. of Health & Human Services, Office of Inspector General (Oct. 27, 2008).

256 *See Randi A.J. v. Long Is. Surgi-Ctr*., 46 A.D.3d 74 (2007 NY Slip Op. 06953) (2d Dept. 2007).

addition, an attorney subpoena is not sufficient to secure an adverse party's records.

Attorneys who need to review medical records or obtain health information in connection with providing legal services or other health operations services for a HIPAA-covered entity do not need a subpoena or authorization to access the information, but do need to enter into a HIPAA business associate contract with the covered entity. The contract imposes on the business associate, *i.e.*, the attorney, the same obligation to protect the confidentiality and security of the information as the covered entity has. In addition, the ARRA amendments make the business associate directly responsible to overseeing agencies for compliance with the security standards and with the provisions of the business associate contract.[257] The HHS Office of Civil Rights has made available a model business associate form,[258] but other versions are widely used as well.

As a general matter, it is good practice to: (i) secure copies of the Office of Court Administration ("OCA") HIPAA authorization forms and a good model HIPAA business associate contract, and become familiar with their requirements; (ii) review the DOH HIPAA preemption chart sufficiently to know the general areas that are subject to conflicting HIPAA and state requirements; (iii) recognize that special protections apply to records maintained by mental health providers and drug and alcohol treatment providers, and to records with HIV/AIDs information and genetic information; and (iv) adhere to clear and strict professional conduct obligations to the maintain confidentiality of client information, which may include client health information.

Attorneys do not have a clear or strict obligation to maintain the confidentiality of the health information of non-clients that they may acquire in the course of litigation or professional

---

257 ARRA §§ 13401(a), 13404(a).

258 http://www.hhs.gov/ocr/hipaa/contractprov.html.

services. However, in such circumstances, regardless of whether or not such obligation is explicit in law or professional conduct guidelines, an attorney should act in a manner as if it were deemed to be a covered entity and should refrain from using or disclosing information obtained in the course of litigation or legal services except for the permissible purposes of the litigation or legal services.[259] Moreover, attorneys are not under any general statutory or regulatory obligation to protect the security of such information.[260] Nevertheless, attorneys who handle medical records should as a matter of professional responsibility, take reasonable steps under the circumstances of their office to protect such records from destruction or inadvertent disclosure, theft and other security breaches.

2. Disclosure of Medical Records and Health Information in Litigation

a. Attorney Access to a Client's Medical Information

There are several ways, as set forth below, in which an attorney may access a client's medical information.

Request with client's HIPAA authorization. The clearest legal basis for an attorney to secure a client's medical record from a provider is to secure a HIPAA-compliant authorization from the client, and present that to the provider with a request for the record. The OCA has developed a HIPAA-compliant authorization form for this purpose, and the form will generally be recognized and honored by providers.[261]

Request with client's non-HIPAA compliant consent. An attorney might also seek access with client's non-HIPAA compliant consent, contending that the attorney is not required to

---

259 *Cf*., *Hageman v. Southwest Gen. Health Ctr*., 2007-0376 (7-9-2008); 2008-Ohio-3343, Supreme Court of Ohio. (Attorney may be liable to an opposing party for the unauthorized disclosure of that party's medical information that was obtained through litigation).

260 However, a lawyer who possesses protected health information as a business associate is subject to the confidentiality and security obligations in the business associate contract. Also, a lawyer who possesses HIV/AIDS information, pursuant to an HIV/AIDS consent is subject to re-disclosure restrictions.

261 *See* www.nycourts.gov/forms/hipaa_fillable.pdf.

produce such authorization because he or she is a "qualified person" under PHL Section 18. That argument might be correct depending upon the circumstances, but it could result in a dispute and delay that would have been averted if the attorney produced a HIPAA authorization.

Client access. An attorney could always have the client request the records directly, under the patient's HIPAA and NYS law right to access his information. Once the client obtains his record/information, he or she is free to disclose it to the attorney.

Requests by a plaintiff for records of their own treatment. New York Civil Practice Laws and Rules ("CPLR") Section 3012-a provides that if a plaintiff requests the records of his own medical or dental treatment by the defendant and such records are not produced, the plaintiff "shall not be required to serve the certificate of merit otherwise required by Section 3012-a."[262]

b. Pre-trial Access to Medical Records and Information About an Adverse Party in a Civil Action[263]

An effort to secure pre-trial access to an adverse party's medical records and information can arise in a wide range of contexts. A defendant's attorney might seek such medical records or information about a plaintiff to help defend a medical malpractice or other personal injury action, or to challenge a worker's compensation claim. Conversely, a plaintiff or petitioner might seek such information about a defendant or respondent in a child custody case, guardianship proceeding, or action to invalidate a will. The principal methods of obtaining such information are as follows:

(a) *Request with adverse party's HIPAA authorization*. A request to a provider with the adverse party's HIPAA authorization will often be sufficient for the provider to produce the medical records. In many instances, the adverse party will be required to provide such authorization to pursue their claim or defense.

---

262 CPLR § 3012-a.

263 This section does not address access to records in criminal actions or the high profile issue of ex parte interviews of treating physicians , and this may be an issue for consideration by future committees. *See Arons v. Jutkowitz*, 9 N.Y.3d 393 (2007).

(b) *Subpoenas.* Under the CPLR, a subpoena *duces tecum* requesting the production of a patient's medical records pursuant to Article 31 (pre-trial disclosure) must be accompanied by the patient's HIPAA authorization, and a provider need not honor it without that authorization.[264] Indeed, the subpoena must state in conspicuous bold-faced type that the records shall not be provided unless the subpoena is accompanied by a written authorization by the patient.[265] Even a subpoena "so-ordered" by the court is insufficient without the required patient authorization.

c. Access to Medical Records and Information For Use at Trial

Although under New York law an attorney subpoena would suffice to compel production of medical documents for trial, HIPAA requirements are more stringent. In general, a court-ordered subpoena is required for such purpose. However, since a subpoena *duces tecum* requesting records for trial is governed by CPLR Article 23, not Article 31, the patient's HIPAA authorization is not required.

3. Privileged Communications

Under the CPLR, a person authorized to practice medicine, registered professional nursing, licensed practical nursing, dentistry, podiatry or chiropractic is not allowed to disclose any information that he or she acquired in attending a patient in a professional capacity, and that was necessary to enable him to act in that capacity, unless the patient waives the privilege.[266] Such waiver must satisfy other applicable HIPAA, other federal and state law requirements. The privilege is designed to "protect those who are required to consult physician from the disclosure of secrets imparted to them, to protect the relationship of patient and physician and to prevent physician from disclosing information which might result in humiliation, embarrassment, or disgrace to patients."[267] The privilege belongs to the patient, not the provider, and if waived by the patient cannot be invoked by the provider.

---

264 CPLR § 3122.
265 CPLR § 3122.
266 CPLR § 4504(a).
267 Steinberg v. N.Y Life Ins., 263 N.Y. 45.

However, with respect to deceased patients, a physician or nurse is required to disclose any information as to the mental or physical condition of a deceased patient that would otherwise be considered privileged, except information which would tend to disgrace the memory of the decedent either in the absence of an objection by a party to the litigation or when the privilege has been waived.[268]

4. Physical or Mental Examination

In an action in which the mental or physical condition or the blood relationship of a party is in controversy, any party may serve notice on another party to submit to a physical, mental or blood examination by a designated physician.[269] The notice may require duly executed and acknowledged written authorizations permitting all parties to obtain, and make copies of, the records of specified hospitals relating to such mental or physical condition or blood relationship.[270] Where a party obtains a copy of a hospital record as a result of the authorization of another party, he or she must deliver a duplicate of the copy to such party.[271]

H. Conclusion: The Future of Health Privacy

Despite the myriad of federal and state statutes and regulations governing the privacy of healthcare information, there are many privacy, security and consent issues that arise with advances in healthcare information technology ("IT"). Among these developments are: (1) the increasing adoption of electronic health records ("EHRs") rather than traditional paper-based medical records; (2) the growth of e-prescribing; (3) the creation of regional health information organizations ("RHIOs"); and (4) the ultimate goal of a National Health Information Network ("NHIN"). Indeed, through the enactment of the ARRA and, specifically, the Health

---

268 CPLR § 4504(c).
269 CPLR § 3121(a).
270 *Id*.
271 CPLR § 3121(b).

Information Technology for Economic and Clinical Health **Act** (the "HITECH Act"), the Obama administration has made the expansion of health IT a major priority. Legislators, regulators, attorneys and healthcare practitioners are increasingly facing the question of how to apply HIPAA and other federal and New York state healthcare laws to these new technological advances.

1. Electronic Health Records

An EHR, sometimes referred to as an electronic medical record, is an individual patient's medical record in a digital format. Typically, an EHR contains a patient's medical history, immunization record, medication information, allergy list, laboratory test results, radiological images like X-rays or MRIs, and advanced directives, if any. EHRs should conform to nationally recognized interoperability standards – meaning that different information systems, software applications and networks are able to communicate and exchange such information in an accurate, effective, useable and consistent manner. EHRs are preferred because they are less expensive, more environmentally sound, and reduce both clinical and billing errors. They are also easier to maintain, keep current and make accessible to healthcare providers.

There can be several clinical benefits of an EHR program. First, all of a patient's medical information is kept in a compact, user-friendly medium – no longer are x-rays or other digital images sticking out of the folder or kept in another location because they do not fit in the patient's file. Second, laboratory results and trends in vital statistics can appear graphically.[272] Third, software can indicate when preventative care is recommended or when adverse reactions may occur. Fourth, clinical errors are reduced due to the elimination of handwriting or transcription errors. Finally, a patient's medical information is readily available to the healthcare

[272] Benjamin J. Beaton, Walking the Federalist Tightrope: A National Policy of State Experimentation for Health Information Technology, 108 COLUM. L. REV. 1670 1676 (Nov. 2008).

professionals treating him or her in a timely, secure and functional manner.

The National Committee on Vital and Health Statistics ("NCVHS") is the public advisory committee to the DHHS on health data, privacy and health information policy. NCVHS, as part of its congressionally mandated functions, oversees the implementation of the existing HIPAA rules and makes recommendations about future additions and modifications to those rules. Since the expansion of NCVHS' charter in 1996, NCVHS has focused on contributing to both DHHS, state and private sector data policy decision-making. NCVHS has focused on the implementation of HIPAA standards – commenting on the administrative process for the development, amendment and update of final federal rules, the areas of data policy that are lacking HIPAA standards, and the need by the OCR to better enforce HIPAA, as discussed above. Most recently, NCVHS recommended streamlining the federal rule development process to expedite the implementation and update of HIPAA standards, and adding HIPAA standards for the collection, storage and transmission of allergy and disability health information, and format and transmission standards of multimedia data. It is unclear at this point, how the passing of the ARRA and the call for a National Coordinator (discussed below) will impact or interact with the activities of NCVHS.

In 2007, NCVHS conducted a hearing and wrote a report on methods of collecting, measuring and reporting hospital performance with respect to quality measurement and data reporting.[273] This Report made ten recommendations that included: (1) promote consistent public reporting of quality measures to promote consumer understanding; (2) support research for improving measurement accuracy and validity; (3) encourage the ongoing development of a set of common data elements for evaluating the quality of care that takes into account the

[273] Letter from Harry L. Reynolds, Jr., Chairman, NCVHS, to Michael O. Leavitt, Secretary, DHHS "Quality Measurement and Public Reporting in the Current Health Care Environment" (Jan. 28, 2007).

increasing availability of computerized clinical data; and (4) accelerate the adoption of electronic health records as an integral part of the quality reporting and improvement functions.[274]

Maintaining a patient's privacy is a legitimate concern with the increased usage of EHRs. In 2006, the *Los Angeles Times* cited a DHHS statistic that approximately 150 people have access to some part of a patient's medical records during a hospitalization.[275] Recent initiatives in which hospital staff wrongly "peeked" at, and even sold, [276] celebrity health information, as well as the increase in identity theft in the financial sector give patients heightened anxiety regarding the electronic storing of their personal medical information. The federal government is taking action to address these concerns and promote the adoption of EHRs. EHRs must be sufficiently protected to maintain, at a minimum, the level of privacy and security afforded paper-based medical records today.

Under Governor Pataki, New York created a statewide grant program known as the Health Care Efficiency and Affordability Law for New Yorkers Capital Grant Program, referred to as "HEAL NY". This program is a multi-year, multi-phased program with two primary objectives: (i) identification and support of the development in health information initiatives in New York; and (ii) identification and support of funding for restructuring regional healthcare plans to improve the quality, efficiency and stability of healthcare in New York. Phase 1 of HEAL NY appropriated $53 million for projects aimed at the implementation of interoperable health information technology systems between unrelated healthcare providers, such as

---

274 10/23/07 Quality Measurement and Public Reporting in the Current Health Care Environment NCVHS Report pages 4-5.

275 Judy Foreman, *At risk of exposure*, L.A. TIMES, June 26, 2006, at F3 *available at* http://latimes.com/2006/jun/26/health/he-privacy26.

276 *E.g.*, "California Hospital Faces Sanctions After Workers Wrongly Looked at Patient Records," NY Times (online) April 8, 2008; Staff Suspended for leaking George Clooney Medical Records, NY Daily News (online) Oct. 10 2007; State Investigates After Leak of Granholm's Medical Records, Grand Rapids Press (online) Aug. 7, 2008); FL Hospital Employees Fired After Peeking at NFL Players Medical Records, FierceHealthcare (online) Nov. 4, 2008.

RHIOs.[277] Phase 5 is currently underway and is focused on advancing interoperability and community-wide EHR adoption in New York. Phase 5 is targeted at RHIOs, community health information technology adoption collaborations, and public-private partnerships.[278] It remains to be seen how the programs and initiatives receiving the grants will cope with consent, privacy and security issues that arise as EHRs become mainstream.

2. Electronic Claims and Billing

Healthcare providers in New York may use electronic claims submission for both Medicare and Medicaid. CMS allows Medicare providers to submit claims electronically to any Medicare carrier, Durable Medical Equipment Medicare Administrative Contractor, or fiscal intermediary by using a computer with software that complies with the electronic filing requirements in the HIPAA transaction standards and Medicare's provider enrollment and certification guidelines.[279] In addition, providers that bill fiscal intermediaries are permitted to submit claims electronically through direct data entry screens. The New York State Medicaid Program also allows electronic claims submissions. Participating healthcare providers must receive an Electronic/Paper Transmitter Identification Number and submit an annual certification statement to the New York State Department of Health. With the widespread acceptance of electronic billing and claims submission comes increased concerns over privacy and security issues. Business associate contracts are one tool used by these contractors, but they may not afford sufficient protection.

3. E-Prescribing

Electronic prescribing of medications, also known as e-prescribing, involves the use of a

---

277 LIPIX, History of Health Information Exchange, *available at* http://www.lipix.org/index.php/Resources.

278 Overview – HEAL NY Phase 5, *available at* http://www/health.state.ny.us/technology/projects/docs/overview.pdf.

279 CMS, Overview Electronic Billing and EDI Transactions, a*vailable at* http://www.cms.hhs.gov/ElectronicBillingEDITrans/.

computer system (*i.e.*, a hand-held device, laptop, or desktop personal computer) by a healthcare provider to electronically transmit data about prescription medications directly to the patient's preferred retail or mail-order pharmacy. In 2007, more than 3.5 billion prescriptions were written to patients in the United States, and it is estimated that the annual number of prescriptions will be over 4 billion by 2010.[280]

The federal government strongly encourages the widespread adoption of e-prescribing by healthcare providers. In 2006, CMS and the OIG promulgated a safe harbor to the Anti-Kickback Statute and corresponding exceptions to the Stark Anti-Referral Act for e-prescribing and EHRs that allow for the donation of electronic health records software or information technology and training services necessary and used predominantly to create, maintain, transmit, or receive electronic health records is permissible if certain conditions are met. Under this new safe harbor, items or services used for e-prescribing must be used solely to receive and transmit electronic prescription information, and for no other purpose, but items or services used for electronic health records systems must be used predominantly to create, maintain, transmit, or receive electronic health records, but may be used for other limited activities.

Beginning January 1, 2009, Medicare offered physician payment incentives of up to two percent for two years to practices that implement certain e-prescribing tools and methods. There is also a potential two percent bonus on physicians' total Medicare allowed charges available under Medicare's Physician Quality Reporting Initiative. The Deficit Reduction Act established Medicaid Transformation Grants to facilitate the reformation of state Medicaid programs, and those funds can be used to finance the "implementation and use of electronic health records,

[280] eHEALTH INITIATIVE, A CONSUMER'S GUIDE TO E-PRESCRIBING 1 (June 2008) *available at* http://www.ehealthinitiative.org/assets/Documents/eHI_CIMM_Consumer_Guide_to_ePrescribing_Final.pdf.

electronic clinical decision support tools, or e-prescribing programs."[281]

NCVHS recently made recommendations for uniform standards governing electronic prescribing in ambulatory care, but these recommendations cannot be acted upon due to the general illegality of e-prescribing controlled substances. This poses a significant barrier to the adoption of e-prescribing generally by providers. NCVHS recently commented to the Department of Justice's notice of proposed rule making regarding the Drug Enforcement Administration's intent to revise its regulations to allow providers the option of writing electronic prescriptions for controlled substances. NCVHS urged the imposition of less onerous security and authentication requirements that balance "security with functionality and clinical practice."[282] Every state, including New York, has a statute allowing pharmacies and physicians to exchange prescriptions electronically. Some regulatory barriers, however, still remain. For example, New York Medicaid rules require that a prescription have "DAW" or "dispense as written" in the physician's handwriting on the prescription pad if the physician does not want the prescription filled with a generic item.

Despite these hurdles, New York recently launched a pilot program known as the Primary Care Information Project ("PCIP") to encourage the use of prevention-oriented EHRs among providers who treat New York City's underserved population. PCIP grants primary care providers who have Medicaid recipients or uninsured represent more than ten percent of their patient population a package of software and services to adopt interoperable EHRs to improve the quality of preventative care for their patients. PCIP teamed up with eClinicalWorks, an EHR and practice management system vendor, to provide selected physicians with the necessary software, applications and licenses, onsite training, and two years of maintenance and support

---

281 42 U.S.C. § 1396b(z) (2008).

282 Letter from Harry L. Reynolds, Jr., Chairman, NCVHS, to Michael O. Leavitt, Secretary, DHHS "Electronic Prescriptions for Controlled Substances" (Sept. 24, 2008).

costs. The program is targeted to Medicaid primary care physicians and practices in Harlem, the South Bronx and Central Brooklyn.[283] According to the New York City Department of Health and Mental Hygiene, as of July 1, 2008, 180 practices in 285 sites with over 1,000 providers signed agreements with PCIP.[284] The goal of the project is to extend prevention-oriented EHRs to at least 2,500 primary care providers and 2 million patients by 2010.[285] Analysis of the privacy and security protections as well as the consent policy in the PCIP – and their effectiveness – will add insight to the optimal structure for EHR programs.

4. Regional Health Information Organizations

a. RHIOs Generally

RHIO is defined as a "health information organization that brings together healthcare stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in that community."[286] A health information organization ("HIO") is an organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards, while health information exchange ("HIE") is the electronic movement of health-related information among organizations according to nationally recognized standards. HIE is a process rather than a structure, and provides the infrastructure necessary for secondary use of clinical data by facilitating access to and retrieval of such health information.

Multiple participants in the healthcare industry form a RHIO to better the quality, efficiency and safety of the healthcare they provide and increase access to healthcare through health information technology. Stakeholders comprising hospitals, health plans, long term care

283 http://www.nyc.gov/html/doh/html/pcip/pcip-summary.shtml.

284 *Id*.

285 *Id*.

286 American Health Information Community, "Defining Key Health Information Technology Terms" http://www.hhs.gov/healthit/documents/m20080603/10.1_bell_files/textonly/slide6.html.

and home care agencies, practice groups, physicians and organizations unite to share data and facilitate collaboration in an effort to benefit each RHIO member. Today, it is estimated that there are more than 150 RHIO-type organizations in existence nationwide.[287]

A RHIO covers a particular geographic area and is typically formed either at the state or local level. Often, states form RHIOs to facilitate the development and operation of regional RHIOs. California's RHIO, known as CalRHIO, is a statewide organization of healthcare providers, payors, public and private organizations that focuses on building a secure statewide HIE system. Increasingly, providers have formed local RHIOs dedicated to a particular geographic region. They serve as neutral coordinators for data exchange among existing healthcare organizations. Most of these are not-for-profit organizations comprised of both public and private members like the Taconic Health Information Network and Community RHIO ("THINC RHIO") and the Bronx RHIO, and they often outsource the exchange services to one of the dozens of EHR software vendors. To date, RHIOs have been slow to develop in rural areas, and it is expected that the federal or state government will take action to foster the creation of RHIOs in rural areas.

There are three generally accepted models for RHIOs: (1) cooperative model; (2) federated model; and (3) hybrid model. The first, a cooperative model, is used mostly by smaller, rural RHIOs that lack significant technological resources and have a strong interest in collaborating. These RHIOs might elect to build a centralized database to store patient health information, thereby sharing the overhead costs and human resources. A RHIO comprised of larger, independent healthcare organizations are more likely to use the federated model because each organization retains its patient data, but shares such information as necessary pursuant to

[287] Press Release, Health Industry Insights, Health Industry Insights Survey Says No Solutions Panacea for RHIO/HIE Organizations (Aug. 7, 2007) *available at* http://www.idc.com/HII/getdoc.jsp?containerId=prUS20818907.

business agreements between the participating entities. This decentralized approach usually results in the RHIO's development of an electronic master patient index that indicates all of the sites where a particular patient's health information is stored. The hybrid, or combination, model is employed mainly by large inter- and intrastate RHIOs that need aspects of both the co-op and federated models.

b. New York RHIOs

The State of New York articulated its definition of a RHIO in its 2007 request for applications to support the statewide HIE adoption. It defined a RHIO as a New York State not-for-profit corporation

> with an overall mission to advance interoperable health IT to improve healthcare quality and safety and reduce costs…RHIOs are responsible for providing key services to advance interoperability, including governance; clinical priorities and effectiveness; technical policies; business model; patient privacy, confidentiality and security policies; and other patient engagement services.[288]

In New York, there are several RHIOs in existence. These include the THINC RHIO, Greater Rochester RHIO, Bronx RHIO, Long Island Patient Information eXchange ("LIPIX"), and the Brooklyn Health Information Exchange. In July 2008, the Bronx RHIO, which covers eighty percent of providers in the Bronx borough, went "live" and began exchanging patient data. The Bronx RHIO is the first "live" RHIO in New York City. According to *Reuters*, as of October 2008, the Bronx RHIO had received consent forms from more than 4,000 patients, and 55 care locations throughout the Bronx were designated as sites where these patients' clinical data may be accessed with appropriate consent.[289]

---

[288] The N.Y. State Dept. of Health and The Dormitory Auth. of the State of N.Y. Request for Grant Applications HEAL NY – Phase 5 Health Information Technology Grants Advancing Interoperability and Community-wide EHR Adoption, Sept. 2007, available at http://www.health.state.ny.us/funding/rfa/0708160258/.

[289] Bronx RHIO First to "Go Live" in New York City; Now Sharing Patient Data From 55 Care Sites,

Aside from funding and technological challenges, the biggest issues facing RHIOs are the privacy and security of the health information. Most RHIOs are building on their predecessors' privacy and security policies. For example, the Tennessee Volunteer eHealth Initiative formed a coalition of eight stakeholders to examine privacy and security approaches based on the Markle Foundation's nine principles for data security.[290] THINC RHIO established seven principles that comprise its consumer privacy and information control policy, and many of them are similar to a healthcare provider's standard HIPAA compliance policy.[291] These guiding principles focus on building consumer trust through maintaining the security and integrity of confidential health information, ensuring accessibility to the THINC RHIO and its administration, and educating consumers on the network, its value, its protections, and its governance.[292]

The RHIO's chosen model also impacts privacy and security concerns. A co-op approach, in which the data is all centralized, increases the potential risk that sensitive information will be improperly disclosed or compromised. First, a centralized database is a more attractive target for hackers. Second, consolidating the data increases the number or organizations and individuals that may need access to the database. The federated model is less susceptible to these risks because organizations enter into formal agreements that specifically identify the access and obligations of each party. RHIOs employing a federated model usually use peer-to-peer requests whereby each provider must use the patient index to determine where the required data is stored and then request the data from the provider who owns and stores such information. Regardless of the approach, the use of security programs and technologies like

---

Reuters, Oct. 6, 2008, available at http://www.reuters.com/article/pressRelease/idUS124709+06-Oct-2008+BW20081006.

290 Heather B. Hayes, *RHIO Confidential*, Govt. Health IT, Sept. 10, 2007, *available at* http://www.govhealthit.com/print/4_12/rhio_report/103625-1.html.

291 THINC RHIO, Inc., Consumer Privacy and Information Control Policy, *available at* http://www.thincrhio.org/doc/ConsumerPrivacyInformationControlPolicy.pdf.

292 *Id*.

those recommended by the HIPAA security standards may enhance the privacy and security safeguards of RHIOs. The HIPAA privacy and security standards, however, do not appear to be readily applicable to RHIOs. Currently, RHIOs are only subject to the HIPAA standards as "business associates"[293] which is just one reason why the NCVHS has advocated applying the HIPAA standards to all healthcare providers. Now, the HITECH Act includes under the definition of "business associate" any entity that provides data transmission services to a covered entity and applies the HIPAA privacy and security requirements to business associates in the same manner as they apply to covered entities. Accordingly, RHIOs will be subject to any implementing regulations of the HITECH Act.

In New York, a complex process has developed for the development of policy and the oversight of RHIOs. Initially, the NYS Department of Health fostered the creation of The New York eHealth Collaborative ("NYeC") to help develop policies, standards and technical approaches for RHIOs, through a "Statewide Collaboration Process."[294] NYeC is composed of the DOH, entities that were awarded HEAL grants for the development of RHIOs, and other stakeholders. More recently, the NYS DOH established an Office of Health Information Technology to coordinate Health information technology programs and policies.

But more specifically with respect to privacy and security issues, DOH created the New York Health Information Security and Privacy Collaborative ("NYHISPC") – another collaborative body with broad multidisciplinary participation.[295] NYHISPC has conducted several conferences and issued various reports on privacy and security issues, including

---

293 Michael D. Greenberg and M. Susan Ridgely, Patient Identifiers and the National Health Information Network: Debunking a False Front in the Privacy Wars, 4 J. Health & Biomedical L. 31, 41 (2008).

294 *See* www.nyehealth.org; www.health.state.ny.us/technology/partnership.

295 *See* www.health.state.ny.us/technology/nyhispc.

"Standardized Consumer Consent Policies and Procedures for RHIOs in New York State."[296] In that report, NYHISPC proposed imposing a standardized consent process for all NYS RHIOs that would include, among its principles, the following:

Affirmative Consent: Each provider organization and payer organization participating in a RHIO must obtain an affirmative consent from the consumer that specifically references the RHIO prior to accessing her/his personal health information.

Up-Loading Data: Health care providers may "upload" patient information to a RHIO without patient consent.

Sensitive Health Information: A single consent may be obtained to exchange all health information, including all specially protected health information.

Consent Form: RHIOs must use a State-approved consent form.

Durability and Revocability: RHIO consents are both durable and revocable.

Consumer Engagement and Access: RHIOs must comply with consumer education, engagement and access standards.

Audits and Transparency: RHIOs must conduct audits at least annually; inform consumers promptly of any breaches and make audit trails available upon request. It is anticipated that online tools and paper-based reports will be utilized.

Enforcement: Consent standards initially will be enforced through contractual relationships between RHIOs and New York State, and should migrate towards requirements for an accreditation process.[297]

Three key issues regarding RHIO's warrant attention:

---

296 http://www.health.state.ny.us/technology/nyhispc/phase_ii/.

297 New York Health Information Security and Privacy Collaboration, Standardized Consumer Consent Policies and Procedures for RHIOs in New York State, December 21, 2007.

(1) "***Opt-in vs. Opt out***": There was considerable debate as to whether consumer consent should be required before their health information was "uploaded" to a RHIO ("opt-in"), or whether the information could be entered without such consent and then consumers would be notified of their right to have their information removed ("opt-out"). Ultimately, as recommended by NYHISPC, New York took a third approach: patient information can be uploaded to a RHIO without consent but it cannot be accessed by providers or anyone else unless and until the consumer consents to access by the provider. In effect, the RHIO can "store" information without consent, but it cannot be used until there is consent. However, RHIOs can "break the glass" to access information without consent in emergencies under certain circumstances.

(2) "***Screening Sensitive Information vs. All-or-Nothing***": NYHISPC had recommended that RHIOs should be able to offer consumers the ability to screen especially sensitive information, such as HIV and reproductive information, from being accessed through the RHIO. However DOH, concerned about the clinical implications of filtering the health information that clinicians see, rejected that recommendation. As a result, while a consumer can provide or decline to provide consent for a provider to access the consumer's information through a RHIO, the decision will encompass "all-or-nothing" of the consumer's health information.

(3) ***Minors:*** Another issue facing New York RHIOs is the treatment of children between the ages of 13 and 17 ("Minors"). Under New York law, certain healthcare services, treatments or tests may be provided to Minors without parental consent. The issue becomes the way in which a RHIO can include a Minor's confidential health information, including protected services, and still ensure that such information is not disclosed to the Minor's parents. Some RHIOs, like LIPIX, will not include any information for children over the age of 10.[298] Others, like the Bronx RHIO, have a hospital emergency department exception.[299]

In late 2008, DOH issued standard forms for providers and payors to use to secure patient consent to their access to health information through a RHIO.

In September 2008, the New York eHealth Collaborative released a white paper

---

[298] Consent for Release of Health Information Through Long Island Patient Information eXchange, *available at* http://www.lipix.org/ConsentForm7-1(1).pdf.

[299] Bronx RHIO, Inc. Policies and Procedures 1-3, Privacy Policy & Procedure p.11 (April 11, 2008), *available at* http://www.bronxrhio.org/downloads/BronxRHIO_PoliciesAndProcedures_April08.pdf.

concerning the potential for accreditation of RHIOs and the benefits for New York's health information technology strategy.[300] Due to the large financial investments made by the local, state and federal government, the New York eHealth Collaborative argues that it is imperative that RHIOs be held publicly accountable. With the expansion of accreditation and deeming agencies across the healthcare industry, it is likely that RHIOs will require accreditation in the future – whether by New York State or the federal government.

c. Nationwide Health Information Network

The NHIN, another initiative of DHHS, is under development to provide a national secure health information network (similar to RHIOs) to connect providers, consumers and other participants in the United States healthcare industry. The NHIN will enable a consumer's health information to follow him, and will increase access to such information by providers for critical decision-making.

The development of the NHIN has raised serious concerns about individual control over a person's private and sensitive health information. While the HITECH Act contains various provisions to address privacy and security concerns, it remains to be seen how the new law and implementing regulations will develop in this area. During the past five years, NCVHS has debated the best approach to guarantee that sufficient privacy protections are included in the NHIN.

In early 2008, the NCVHS wrote to DHHS Secretary Michael O. Leavitt and recommended that the NHIN allow each individual limited control over such person's sensitive

[300] New York eHealth Collaborative. Interoperable Health Information Exchange Policy, Governance, and Accountability: Examining the Potential Role for RHIO Accreditation in New York's Health Information Technology Strategy. Sept. 2008. available at http://www.nyehealth.org/files/File_Repository16/pdf/NY_RHIO_Accred_Paper.pdf.

health information.[301] Specifically, NCVHS advocated the categorization of health information into sensitive, or more highly protected categories, such as genetic information, substance abuse, domestic violence, mental health information, and reproductive health. Many of these categories of sensitive health information receive special treatment under New York privacy laws, as discussed above. NCVHS suggested that individuals have the ability to sequester certain categories of sensitive health information, and have a corresponding note added to his/her medical record on the NHIN that certain information has been blocked. NCVHS did not determine whether a general notice that some sensitive health information had been sequestered or a notation identifying the affected category or categories was a better approach. Finally, NCVHS provided for a "break the glass feature" in emergency situations in which a patient is unable to give or refuse consent to access sequestered information. This would allow a provider to have access to all of that individual's health information, but NCVHS recommended that there be an audit trail and review by a privacy officer, and the re-sequestration of the sensitive health information.

As discussed above, New York is taking a different approach with respect to sensitive health information maintained in regional health information systems. It is unclear how, if at all, the NHIN and RHIOs will work together.

It has been estimated that an NHIN could necessitate $156 billion in capital investments over five years and would incur $48 billion in annual operating costs.[302] The widespread development of RHIOs could trim these costs. RHIOs determine how patients' health

---

301 Letter from Simon P. Cohn, M.D., M.P.H., Chairman, NCVHS, to Michael O. Leavitt, Secretary, DHHS "individual control of sensitive health information accessible via the Nationwide Health Information Network for purposes of treatment" (Feb. 20, 2008).

302 Kaushal, R., Blumenthal, D., Poon, E.G., Jha, A., Franz, C. Middleton, B., Glaser, J., Kuperman, G., Christino, M., Fernandopulle R., Newhouse, J.P., Bates, D.W., and The Cost of National Health Information Network Working Group. (2005). The Costs of a National Health Information Network. Annals of Internal Medicine 143, 3: p. 166.

information is shared within that geographic area, and these RHIOs will eventually connect to state, multi-state and ultimately national networks, but RHIOs are developing organically with different methods across the country and they may not unify seamlessly. Experts argue that RHIOs will help eliminate some of the administrative costs associated with paper-based patient records, provide faster access to test results, and offer a more complete picture of a patient's medical history. Furthermore, President Obama has made HIE and improving "information technology at hospitals and doctors' offices" a part of his public works program to resuscitate the U.S. economy.[303]

As of February 14, 2008, when Valerie Melvin of the U.S. Government Accountability Office testified before the Senate Committee on the Budget, there does not appear to be a clear national strategy for the implementation of HIOs and HIE.[304] A standardization or certification processes for EHR software and products as well as national privacy and security standards for health information technology may be needed.

5. Current Legislative Environment

Health information technology and use of electronic medical records networks signify marked advances in the delivery of healthcare. However, the use of electronic medical records exchanges has created increased debate over the past several years as to whether existing federal and state healthcare privacy and security rules are effective in protecting the privacy of patients in today's healthcare environment.

In recent years, Congress has examined health technology and related privacy legislation

---

303 Peter Baker and John M. Broder, *Obama Pledges Public Works on a Vast Scale*, N.Y. TIMES, Dec. 7, 2008, *available at* http://www.nytimes.com/2008/12/07/us/politics/07radio.html?_r=1&ref=todayspaper.

304 Health Information Technology: HHS Is Pursuing Efforts to Advance Nationwide Implementation, but Has Not Yet Completed a National Strategy: Testimony Before the S. Comm. On Budget, 110th Cong. (2008) (statement of Valerie C. Melvin, Dir. Human Capital and Mgmt. Info. Sys. Issues, U.S. G.A.O).

intended to promote the use of health information technology and create an appropriate regulatory framework for this development. According to the Healthcare Information Management Systems Society,[305] approximately forty-one pieces of legislation related to health information technology were introduced by the 109th Congress, and to date, approximately twelve bills and reports were introduced by the 110th Congress. These bills cover a wide range of topics relating to health information technology, including, but not limited to: (i) grants and financial assistance for the development and implementation of health information technology systems; (ii) standards for health IT exchanges; (iii) incentives to healthcare providers for using health IT; and (iv) provisions addressing the privacy and security protections of electronic health information.[306]

Certainly, the most significant piece of legislation to pass addressing health IT exchanges and related privacy and security issues is the HITECH Act. The HITECH Act, among other things, advances the use of health information technology by: (i) requiring the government to take a leadership role to develop standards by 2010 which allows for the nationwide exchange and use of electronic health information; (ii) investing $20 billion in health IT infrastructure and Medicare and Medicaid incentives to encourage healthcare providers to share electronic health information; and (iii) strengthening federal privacy and security law to protect identifiable health information from misuse as the healthcare sector increases the use of health IT.

In addition to the new HIPAA privacy and security requirements on health plans, business associates and other vendors or personal health records discussed above, the new law

---

305 The Healthcare Information Management Systems Society is a health industry membership organization that is focused on providing leadership with respect to the use of health information technology and management systems to improve healthcare. Each year, it maintains a list of health information technology legislation introduced in Congress, including the status of the legislation.

306 U.S. Government Accountability Office, Health Information Technology: HHS Is Pursuing Efforts to Advance Nationwide Implementation, but Has Not Yet Completed a National Strategy (2008).

includes appropriations for health IT and new health IT requirements for the government sector or businesses who have government contracts. Federal agencies that implement, acquire or upgrade health IT systems to use systems and products that meet certain security standards, and healthcare payers and providers that contract with the federal government must use health IT standards and products that meet these new standards as well. Interestingly, the new law expressly provides that these new standards would be voluntary for private entities.

The HITECH Act codifies the Office of the National Coordinator for Health Information Technology (ONCHIT) and requires the Secretary to appoint a National Coordinator for ONCHIT. The National Coordinator will be responsible for health IT policies and programs, developing a voluntary health IT certification program, and setting milestones for utilization of EHRs for each person in the United States by 2014. It is unclear at this point how ONCHIT will work with NCVHS and its current programs and activities.

With the advancement of health information exchange networks and the use of electronic health records comes a need to ensure appropriate safeguards with respect to the privacy and security of such information. While the HITECH Act contains various provisions aimed at improving and expanding current federal privacy and security protections for health information, the extent and sufficiency of these protections remains to be seen.

IV. KEY PRIVACY ISSUES IN EMPLOYMENT LAW

A. Introduction

A significant, but exceedingly patchwork-like, body of federal and state statutory and case law governs the often conflicting interests of employers, employees, and the unions who represent employees in the privacy and confidentiality of information about individual employees, information provided by individual employees to their employers, and information deemed sensitive and confidential by employers. To name a few of these sources of law we refer to such federal statutes as the NLRA, HIPAA, the Family and Medical Leave Act, the Americans with Disabilities Act, the Pregnancy Disability Act, the Age Discrimination in Employment Act, the ECPA of 1986 and the Employee Polygraph Protection Act of 1988, as well as various New York State statutes, including the Information Security Breach and Notification Act, the New Social Security Number Protection Law, the Disposal of Personnel Records Law, the Security Freeze Law, the New York Wiretapping Law and the New York Lawful Recreational Activities Law. In the area of public sector employment, we can add the Constitutions of the United States and the State of New York, the Civil Service Law, and numerous regulations, ordinances and local laws promulgated by State agencies, city agencies, counties, county agencies, school districts, and other public employers. To the extent privacy issues arise out of harassment in the workplace and employer attempts to investigate it, or employer efforts to probe certain personal information concerning employees or applicants for employment or their lifestyles or family lives, protections can be found, as well, in various federal and state statutes such as Title VII of the Civil Rights Act, the Age Discrimination in Employment Act, the Americans with Disabilities Act, the Taylor Law, the New York State Human Rights Law, the New York City Human Rights Law, and judicial constructions of those statutes. In the financial services industry, drug testing is routine and expected, employers are required to fingerprint and obtain

criminal history records concerning many employees, and SEC regulation *require* the monitoring, recording, and storage of employee e-mails and voice mail communications. Further, where there are special circumstances, as with respect to immigration or occupational health and safety issues arising in the workplace, or record retention and disclosure issues, these and other statutes also offer other protections to employees, impose responsibilities on employers, and impose proscriptions on both.

Indeed, the very notion of "privacy" in the workplace is so exceedingly contextual that it is difficult to conceive of a one-size-fits-all definition of privacy that would be useful or applicable to the entire universe of workplaces in our State. The concept of "privacy" in highly regulated places, such as the financial services industry referred to in the last paragraph above, is likely a much different legal creature from the concept of "privacy" in a hospital workplace, which in turn may well be entirely different from the "privacy" that it is reasonable for an office worker or a construction worker to expect at the workplace. Moreover, to the extent aspects of these statutes and the body of law interpreting them described above are in developing stages, that may be a reflection not only of new and rapidly evolving technology and our changing use of and exposure to that technology, but of our need to adjust to the particular problems created by this technology as it emerges.

Equally important in this context is the need to recognize the role society has assigned the employer. As seen below, the law charges employers with responsibility for private conduct that occurs among employees *inter se*, as well as between employees and their supervisors; for communications between employees and third parties; and for protecting and maintaining the confidentiality of certain private information of its employees, vendors and customers. The extent to which employers are held liable in such circumstances creates a great deal of conflict

between an employer's desire to know, and even for its obligation to obtain and maintain, information concerning its employees on the one hand, and employee's equally strong desire to keep the employer from learning in the first place on the other.

This section of the Report surveys some of the statutes that have been enacted in New York State that address some of these issues, as well as other issues relative to privacy concerns and the relative rights and obligations of employers and employees. However, what follows in this initial overview is not, by any means, an exhaustive survey or analysis of existing statutory or other authority, but merely a preliminary assessment of the types of data and monitoring issues of privacy in the workplace addressed by statutory regulation. It is the view that more work remains to be done in order to establish a comprehensive survey of the statutes and judicial doctrines that are relevant in this area, as well as of the policy issues they raise.

B. Constitutional Protections

The Fourth Amendment to the United States Constitution and similar state constitutional provisions prohibit unreasonable searches and seizures by the government. Such search and seizure restrictions can be found in Article I, Section 2, of the New York State Constitution. In general, the New York courts apply an analysis similar to that applied in the federal context.

One question that is often central to claims of unconstitutional invasions of privacy in a government workplace or in a private workplace by government actors is whether the plaintiff employee enjoyed a reasonable expectation of privacy.[307] A reasonable expectation inquiry generally entails two considerations: whether the individual's conduct "exhibited an actual

---

[307] *See, e.g., Mancusi v. DeForte*, 392 U.S. 364, 88 S. Ct. 2120 (1968) (union official had standing to challenge constitutionality of search of union office he shared with other union personnel that was conducted by officials who served a subpoena *duces tecum* which had been issued by district attorney without a search warrant, notwithstanding that the seized papers were the property of the union, where union official reasonably could have expected that only his union superiors and their personnel or business guests would enter the office and where the union had objected to the search).

(subjective) expectation of privacy"; and whether that subjective expectation is "one that society is prepared to recognize as 'reasonable.'"[308] While the prohibition on governmental searches and seizures extends to private business premises expectations of privacy generally are recognized to a lesser extent in commercial premises than in an individual's home.[309] Note that there is no constitutional prohibition against searches and seizures by private employers conducted in private sector workplaces, although depending on the particular circumstances, a private employer acting under color of federal or state law or regulations or at the direction of government officials may be held to the constitutional standard that applies to and restricts government searches and seizures.

C. Workplace Privacy: The Difficulty of Defining It

In addressing issues of employer monitoring of employee conduct and communications in the workplace, the issue of "privacy in the workplace" is not easily defined, largely because of the highly contextual nature of this concept – as noted above, what is a reasonable expectation of privacy in one workplace (*e.g.*, the financial services industry) may be much different in other kinds of workplaces (*e.g.*, office environments, health care workplaces, retail operations, and construction sites). Moreover, the conflicting interests of employer and employee add further to the difficulty of defining what "privacy" means in the workplace – the employer owns the workplace and the electronic equipment by which employees engage in communications that they wish to be treated as private and outside the scope of legitimate employer access and/or monitoring. In addition, the interests of employees in the privacy of communications with or from their co-workers are often in conflict (*e.g.*, the male employee who thinks he is courting a

---

[308] *Smith v. Maryland*, 442 U.S. 735, 99 S. Ct. 2577, (1979) (quoting Justice Harlan's concurring opinion in *Katz v. U.S.*, 389 U.S. 347, 88 S. Ct. 507 (1967)).

[309] *See New York v. Burger*, 482 U.S. 691, 107 S. Ct. 2636 (1987); *Donovan v. Dewey*, 452 U.S. 594, 101 S. Ct. 2534 (1981).

female employee with e-mails that compliment her attributes and make inquiries into her personal life may regard those communications as warranting a different degree of protection as "private" communications than the female recipient of those communications who regards them as workplace harassment that the employer should know about and stop). Nonetheless, any notion of "privacy" in the workplace must take account of the interest that individual employees have in freedom from unwarranted intrusions.

Generally, where recognized, the tort of invasion of privacy is based upon "an unreasonable intrusion upon the seclusion of another"[310] In the workplace, however, the intrusion may be by a fellow employee, a manager, a supervisor, a co-worker, or others – and it may invoke any one of a number of concerns that the intrusion in some way creates or remedies a hostile work environment. A definition that would separate the reasonable intrusion from the unreasonable intrusion in the private sector workplace would have to take account of whether the intrusion by one employee threatens, harasses, or otherwise undermines the safety, health, production, productivity, personal rights, confidentiality of information, morale or integrity of other employees, and whether the intrusion constitutes unlawful discrimination or retaliation. It also would have to address other legitimate business considerations of the employer, including the rights of vendors, customers or others with whom the employer deals, as well as the employer's property interests in the use of and access to the employer's own communications equipment or devices. In addition, the right of employees to organize unions free from employer coercion also has to be weighed. The complexities are such that issues ranging from violence to romance or nepotism in the workplace, sometimes arising or even occurring away from the workplace, may be the basis for inquiries or observations of employee conduct that the employee would contend are outrageously unreasonable but which the employer would contend are not

[310] Section 652B, Restatement (Second) Torts.

only entirely reasonable but also compelled as a matter of meeting the employer's obligations under the law.

An employer's duty may require monitoring employee activities or acting as a censor in the workplace. At the same time, the employer's effort to monitor or otherwise investigate may, in and of itself, be characterized by those being monitored or investigated as an unwarranted intrusion for which an injunction and or damages may be sought. As yet there is no meaningful definition of what "privacy in the workplace" is.

D. Electronic Data

Widespread use of computers and other electronic devices, as well as the Internet, have dramatically altered and expanded the landscape of today's workplace. Whether because of the decreased amount of personal time available in today's society, because of the manner in which people communicate today and/or because of the changes in our mores, many employees and employee advocates believe that some degree of personal Internet or other electronic communication use in the workplace should be permitted, and that their employers should not have the right to monitor such communications or the sites they visit. While many employers believe a reasonable amount of personal use for understandable purposes is not only acceptable but also contributes to employee morale, many employers and employer advocates believe that unrestricted employee use of the employer's electronic devices at, or even away from, the workplace is highly problematic.

A recent CareerBuilder.com survey,[311] for example, reports the following statistics on personal Internet usage at the office:

- 61 percent of workers surveyed use the Internet for non-work related research and activities (37 percent spend average of more than 30 minutes per day; 18 percent

[311] Twenty-Nine Percent of Workers Holiday Shop Online While at Work, Finds Annual CareerBuilder.com Survey, N.Y. Times, Nov. 25, 2008.

spend average of an hour or more);

- 20 percent of workers surveyed send six or more non-work related e-mails per day;
- 9 percent of workers have a personal blog (23 percent spend time blogging at work; 9 percent spend 15 minutes or more blogging during work day);
- 41 percent of workers surveyed have a social network page (35 percent spend time on their social networking page during work; 8 percent spend 30 minutes or more); and
- 20 percent of workers surveyed use instant messenger at least once a week.

In another survey, 20% of working Americans polled volunteered that they used such electronic devices to engage in sexually explicit online activity such as visiting pornographic web sites.[312] Further, the more employees use the Internet for these and other personal reasons, the greater the likelihood they will be barraged with unsolicited e-mails and related information of all kinds, including of a pornographic nature, and the greater the likelihood certain of those communications will be forwarded to fellow employees. The potential for a hostile work environment, and the disruption and liability it may bring, is real.

If there is any doubt about the extent to which such electronic communications have become a focal issue in the workplace, that doubt quickly melts away in the face of the extent to which such electronic communications are used as evidence both to support and to disprove employee claims, not only as to sexual and other forms of harassment, but also as to claims of discrimination based on race, gender, age, disability and other prohibited characteristics, retaliation, defamation, whistleblowing, breaches of restrictive covenants and other statutory, contractual or tort causes of action. Such evidence may demonstrate a particular timeline or for other purposes and has been deemed "publication" for purposes of asserting a cause of action in

---

[312] "*Sex In The Workplace: Employment Law Alliance Poll Finds 24% Involved In Sexually-Explicit Computing,*." News & Article Library, 10 Feb. 2004 (updated 16 Apr. 2007); Employment Law Alliance, 22 Dec. 2008 http://www.employmentlawalliance.com/en/node/1324.

defamation.[313]

In the same vein, if an employer is to protect itself and its employees, it must guard against improper employee use of electronic communications, including for purposes of quality control and productivity, to investigate criminal or other types of misconduct or wrongdoing, or simply to defend itself, or its employees, against any claims asserted. Indeed, these types of issues have totally transformed, and too frequently dominate, the litigation landscape. Courts and attorneys now regularly struggle with the difficult issues and costs associated with the preservation and discovery of information so commonplace to the electronic workplace.[314]

In *Leventhal v. Knapek*,[315] the court was faced with these issues in a suit by a New York State Department of Transportation employee who, the court found, "had some expectation of privacy in the contents of his computer."[316] Notwithstanding that expectation, the court, citing *O'Connor v. Ortega*,[317] concluded that the searches were reasonable in light of the DOT's need to investigate the allegations of the employee's misconduct as balanced against the modest intrusion caused by the searches.[318]

1. Attorney-Client Privilege And Work Product Doctrine

Issues of attorney-client privilege and the work product doctrine relative to an employee's use of his or her employer's electronic equipment and the expectation of privacy may arise both in the public and private sectors. This is an important and evolving issue.

---

313 *See, e.g.*, *Meloff v. New York Life Ins. Co.*, 51 F. 3d 372 (2d Cir. 1995) (internal e-mail, identifying "subject" as "fraud" and describing termination of employee due to misuse of credit card, stated cause of action in defamation).

314 See, e.g., West v. Goodyear Tire & Rubber Co., 167 F. 3d 776, 779 (2d Cir. 1999); Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998), overruled on other grounds, Rotella v. Wood, 528 U.S. 549, 555 (2000); Zubulake v. UBS Warburg LLC, 2003 U.S. Dist. LEXIS 18771 (S.D.N.Y. October 22, 2003).

315 *Leventhal v. Knapek*, 266 F. 3d 64 (2d Cir. 2001).

316 *Id*. at 66 (government employee occupied a private office with a door, had exclusive use of computer, desk and filing cabinet in his office, and no evidence that visitors or the public had access to his computer).

317 *O'Connor v. Ortega*, 480 U.S. 709 (1987).

318 *Id*. at 66, 73.

Section 4548 of New York's Civil Practice Laws and Rules provides, "No communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication." That provision notwithstanding, in *Scott v. Beth Israel Med. Ctr.*,[319] the court denied the plaintiff's motion for a protective order requiring the defendants to return all e-mail correspondence between him and his attorney, even though the communications had been earmarked as confidential and for the use of the addressee and had specified that all copies must be erased and the plaintiff's law firm notified immediately of any dissemination. The court found that the employer had communicated a policy to its employees which barred personal use of the employer's email system and put them on notice that the employer could monitor all use of the system. The court held that it was therefore clear that the plaintiff could have be no reasonable expectation of privacy in personal communications made on the system, including communications with counsel.[320] Further rejecting the employee's argument as to attorney work product, the court determined a pro forma legend of privilege on an e-mail communication was insufficient precaution to override the likelihood of dissemination under the employer's policy.

2. Statutory Limitations on the Employer's Right to Monitor

a. Electronic Communications Privacy Act of 1986 ("ECPA")

Congress enacted the ECPA to afford privacy protection to electronic communications. Title I of the ECPA amended the federal Wiretap Act[321] which previously addressed wire and oral communications only. Title II of the ECPA created the Stored Communications Act

319 *Scott v. Beth Israel Med. Ctr.*, 17 Misc. 3d 934, 838 N.Y.S.2d 436 (New York County 2007).
320 Id.
321 18 U.S.C. §§ 2510–22.

("SCA")[322] in order to address access to stored wire and electronic communications and transactional records. Both the Wiretap Act and the SCA were amended by the USA PATRIOT Act,[323] to allow law enforcement authorities easier access to electronic communications.

(i) Conduct Prohibited under the ECPA

Under the ECPA, the intentional and unauthorized interception and access of any wire, oral or electronic communication (which includes e-mail communications) is prohibited, as is the disclosure of any intercepted communication.[324] The prohibition against interception protects only the content of the communication, however, so information such as the names of the parties to a communication and the time and length of a communication are not subject to ECPA protections.[325]

Under the ECPA, an employer may monitor business-related phone calls with a telephone extension, switchboard, or other telephone component if the monitoring is done in the ordinary course of business to evaluate performance, train employees, etc. Such monitoring likely falls within the extension telephone and ordinary course of business exceptions to the ECPA. Nevertheless, absent employee consent, even monitoring for a business purpose may violate the New York Wiretapping Law. Monitoring of personal telephone calls, however, will not fall

322 18 U.S.C. §§ 2701–12.

323 Pub. L. No. 107-56, 115 Stat. 272 (October 26, 2001).

324 18 U.S.C. § 2510 *et seq.*, § 2701 *et seq.*

325 *See* 18 U.S.C. §§ 2510, 2511; *see Fraser v. Nationwide Mutual Ins. Co*., 352 F.3d 107 (3d Cir. 2003) (company's access of insurance agent's e-mail without his express permission was deemed not to be an illegal "intercept"; while company's main file server could arguably be considered "backup storage" under the ECPA, company's actions were protected under the exception applicable to "the person or entity providing a wire electronic communications service" because, as the provider and administrator of the e-mail service, company was entitled to protection for all searches of e-mail stored in its system); *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868 (9th Cir. 2002) (in order for a web site such as the employee's to be "intercepted" in violation of the ECPA, it must be acquired during transmission, not while it is in electronic storage; here, pilot created and maintained secure web site that posted information criticizing company, its officers and the airline pilots union, and access to web site was controlled by requiring visitors to log-in with a user name and password; supervisor's viewing of the web site was not "interception" because information was in electronic storage).

within the ECPA ordinary course of business exception. Such monitoring may be permissible under the ECPA and the New York Wiretapping Law only with employee consent.[326]

(ii) Exceptions

Several statutory exceptions to the ECPA are relevant in the employment context.

- Consent – A communication may be intercepted or reviewed if at least one party to the communication has given prior express or implied consent to the monitoring or accessing of the communication, as long as the communication is not intercepted for the purpose of committing a criminal or tortious act.[327]

- "Provider" exception – If the employer is a system provider under the ECPA, it may intercept e-mail where the interception is done during the ordinary course of business and is either (1) "a necessary incident to the rendition of [ ] service" or (2) necessary "to the protection of the rights or property" of the employer-provider.[328]

- "Stored communications" exception – The person or entity providing a wire or electronic communications service may monitor stored communications.

- "Ordinary course of business" exception – If the interception occurs in the ordinary course of the employer's business and is accomplished through the use of equipment furnished to the employer by a "provider of wire or electronic communication" in the ordinary course of the provider's business, the interception is permissible under the ECPA. Cases construing this exception have involved telephone rather than e-mail monitoring; the language of the statute suggests that e-mail communications may not be covered by this exception.[329]

(iii) Penalties

The ECPA permits private causes of action and authorizes recovery of punitive damages and attorneys' fees. The ECPA provides for both civil and criminal penalties.

A violator found liable in a civil action is responsible to the aggrieved party for the greater of either: (i) actual damages suffered by the party, in addition to any profits made by the

---

326 *Williams v. Poulos*, 11 F.3d 271 (1st Cir. 1993) (employer's interception of corporate officer's telephone calls was deemed outside the consent exception to the ECPA where, although officer was told that employee calls would be monitored, officer was not told the manner in which they would be monitored, nor was he told that he would be subject to monitoring); *Deal v. Spears*, 980 F.2d 1152 (8th Cir. 1992) (employee's consent to tape recording or interception of telephone calls cannot be implied merely because employer warned employees that calls may be monitored to cut down on personal use of the telephone; for consent to be implied, employer must notify employees that telephone calls will be monitored).

327 *See* 18 U.S.C. §§ 2511, 2701.

328 *See* 18 U.S.C. § 2511.

329 *See* 18 U.S.C. § 2510.

violator; or (ii) statutory damages, which have been defined as the greater of either $10,000 or $100 per day for each violation. In some circumstances, the ECPA also permits the recovery of additional civil damages, such as preliminary, equitable or declaratory relief, punitive damages and/or reasonable attorneys' fees and litigation costs.

A violator found guilty on criminal charges under the ECPA may be fined up to $5,000, be imprisoned for not more than five years, or both.

b. State Communications Restrictions

Many states have laws that are similar to the ECPA, but more restrictive.

(i) New York Penal Law Section 250 *et seq.* (The New York Wiretapping Law):

(a) Under Section 250 of the New York Penal Law, wiretapping (the intentional overhearing or recording of a telephonic or telegraphic communication by someone other than the sender or receiver without consent), and the interception or accessing of electronic communications, including e-mail, are Class E felonies.

(b) The monitoring, interception and disclosure of e-mail communications is permitted only with the express or implied consent of one of the parties to the transmission.

(c) The New York Wiretapping Law does not contain the "extension telephone" or "ordinary course of business" exception contained in the federal law.

(d) The New York Wiretapping Law has not been construed to allow private causes of action.

(ii) New York Penal Law Section 250.25. Under this section of the Penal Law, a person is guilty of tampering with private communications when "[k]nowing that he or she does not have the consent of the sender, he or she opens or reads a sealed letter or other sealed private communication." Divulging such information to third parties is also prohibited.

Electronic communications, however, are by their nature not private. They are often analogized to postcards.

E. Statutory Protections of Employee Information

1. Privacy Under the New York Civil Rights Law

a. NY Civil Rights Law Section 50

The use of a living person's name, portrait or picture for purposes of advertising or trade without the person's written consent, or the consent of parent or guardian of a minor is a misdemeanor.

b. NY Civil Rights Law Section 50-a

All personnel records used to evaluate performance toward continued employment or promotion of police officers, correction officers, peace officers and firefighters, under the control of their respective agencies, are confidential and not subject to inspection without the written consent of the individual except as mandated by a lawful court order. Such a court order will not be issued "without a clear showing of facts sufficient to warrant the judge to request records for review," and only after the judge reviews such request and gives interested parties the opportunity to be heard. If after the hearing the judge finds sufficient basis, he or she shall sign an order that the personnel records be sealed and sent directly to him or her. The judge will review the file and make available those parts of the record found to be "relevant and material." These provisions do not apply to the district attorney and other public attorneys, a grand jury or any agency of government requiring the documents in the furtherance of their official functions.

c. N.Y. Civil Rights Law Section 50-b

The identity of any victim of a sex offense or any offense involving the alleged transmission of HIV shall be confidential. Any document, picture or photograph, or part thereof, in the possession of any public officer or employee which identifies such a victim shall not be made available for public inspection. This provision does not prohibit disclosure to any person charged with the commission of an offense against such victim; the counsel or guardian of such

person; the prosecutors, investigators or necessary witnesses of either party; or any person who can demonstrate to a court having jurisdiction that good cause exists for disclosure to that person; or a person or agency upon written consent of the victim. This section shall not be construed to require the court to exclude the public from any stage of a criminal proceeding.

d. N.Y. Civil Rights Law Section 50-c

If the identity of a person described in Section 50-b is disclosed in violation of the section, the person injured may bring an action to recover damages suffered by reason of the wrongful disclosure. The court may award attorneys' fees to a prevailing plaintiff.

e. N.Y. Civil Rights Law Section 50-d

Personnel records of court officers used to evaluate performance toward continued employment or promotion can be disclosed in a court action only after the court has notified the subject of such record and has given him or her the opportunity to be heard on the question as to the whether the records are relevant and material in the action before the court. Only the portion found relevant and material will be made available. This provision does not apply to any grand jury or government agency which requires the records in the furtherance of their official duties.

f. N.Y. Civil Rights Law Section 50-e

This is the same as Section 50-d but is applied to the personnel records of bridge and tunnel officers, sergeants and lieutenants.

g. N.Y. Civil Rights Law Section 51

This section applies to a person whose name, portrait, picture or voice is used within this state for purposes of advertising or trade without that person's written consent. Such a person may maintain an equitable action in the Supreme Court to prevent and restrain the use thereof and may sue and recover damages for any injuries as a result of activity found to be unlawful under Section 50 of this article. Nothing in this article shall prevent the sale or transfer of such

name, portrait, picture or voice in whatever medium to any user in a manner that is lawful under this article. Nothing in this article shall prevent a person, firm, or corporation in the photography profession from exhibiting a work unless a written notice objecting to such use is sent by the person portrayed. Nothing shall prevent a person, firm, or corporation from the sale or transfer of such name, portrait, picture, or voice to any user of the information, or for sale or transfer directly to third parties, for use in a manner lawful under this article. This article also does not prevent any person, firm, or corporation from using the name, portrait, picture, or voice of any manufacturer or dealer in connection with the goods, wares, or merchandise manufactured, produced or dealt in by him or her which he or she has sold or disposed of, or from using the name, portrait, picture or voice of any author, composer or artist in connection with his or her literary, musical or artistic production which the manufacturer has sold or of which he or she has otherwise disposed. This section also shall not prevent a copyright owner of a sound recording from disposing of, dealing in, licensing or selling that sound recording if the copyright owner has the right to do so under legal contract conferred from such living person or the holder of such right.

2. Identity Protection in New York

a. The New York State Consumer Protection Board recently published a Business Privacy Guide to help business owners better understand the importance of protecting customer and employee personal information and some of the applicable laws.[330] As there indicated, New York has the second highest number of data breach incidents in the country and is sixth per-capita in identity theft complaints, and identity theft by itself cost businesses over $40 billion in 2007. Such personal identifiable information that businesses collect and

[330] http://www.consumer.state.ny.us/pdf/the_new_york_business_guide_to_privacy.pdf.

retain include names and addresses, Social Security numbers, credit and debit card numbers and individual account or bank numbers.

b. As discussed briefly in Section V. herein, the New York Social Security Number Protection Law[331] became effective January 1, 2008 and prohibits any person or firm from doing the following with a Social Security number and any number derived from it:

- Making a Social Security number available to the general public in any manner;
- Printing an individual's Social Security number on a card or tag used to access products, services or benefits;
- Requiring an individual to transmit his or her Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted;
- Requiring an individual to use his or her Social Security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required;
- Printing an individual's Social Security number on any mailed materials unless required by state or federal law (Social Security numbers may be included in application or enrollment documents to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the number).

The following prohibitions become effective January 3, 2009:

- Encoding or embedding a Social Security number in or on a record or document by using a bar code, magnetic strip or other technology;
- Filing a document available for public inspection with any state agency or political subdivision, or in any court that contains a Social Security number, unless by consent or as required by federal or state law.

c. The New York Employee Personal Identifying Law[332] went into effect on January 3, 2009. Employers require to must create policies and procedures to protect against violations of this section and give notification to employees of such policies and

[331] N.Y. Gen. Bus. Law § 399-dd.
[332] N.Y. Gen. Bus. Law § 399-dd.

procedures or it will be presumed that any violation which occurs is knowing. Under this law an employer shall not, unless otherwise required by law:

- Publicly post or display an employee's Social Security number;
- Visibly print a Social Security number on any ID badge or card, including a time card;
- Place a Social Security number in files with unrestricted access;
- Communicate an employee's personal identifying information to the general public (includes Social Security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage or driver's license number).

d. The New York Disposal of Personal Records Law[333] concerns the destruction of business records that contain personal identifying information (including Social Security number, driver's license number or ID number, mother's maiden name, financial services, checking or debit account numbers or codes, ATM code).

e. The Information Security Breach and Notification Act[334] requires a business to notify affected customers and the proper authority when an unauthorized party has accessed computerized data containing "private information" which is defined as a name or other identifier in combination with a Social Security number, driver's license, or an account, credit or debit number. As stated in the law, the "disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement…."

[333] N.Y. Gen. Bus. Law § 399-h; *see also* Section V., *infra.*
[334] N.Y. Gen. Bus. Law § 899-aa; *see also* Section V., *infra.*

3. Employee History

a. Arrest and Conviction Record

It has been recognized in New York for many years that an automatic personnel decision based on a criminal record is unacceptable, due to the adverse impact of such a policy on members of minority communities. Decisions based on such factors are subject to close scrutiny and require a sufficient showing of a 'business necessity" to justify. However, it may be lawful for an employer to screen out candidates with criminal records who were convicted of a type of offense that would render them inappropriate for the particular position at issue. It should be noted that in New York employers may not inquire about arrests or criminal accusations that did not result in conviction, unless the arrest is pending at the time of the inquiry.[335] Furthermore, in New York, candidates convicted of a crime and denied employment may demand, within thirty days, a written statement explaining why they were denied employment.[336]

b. Litigation History

An inquiry of an employer into an applicant's history of making discrimination complaints against a prior employer may be viewed as evidence of retaliation in violation of federal and state anti-discrimination statutes, if the applicant is not hired.[337]

c. Financial Information

As discussed in more detail in Section V., *infra*, the Fair Credit Reporting Act requires an employer who retains a third party to collect information about an employee or prospective employee to follow certain steps. The Act requires an employer to:

---

335 N.Y. Exec Law § 296(16).

336 *See, e.g.*, N.Y. Correction Law § 754.

337 *See Barela v. United Nuclear Corp.*, 462 F. 2d 149 (10th Cir. 1972) (affirming the judgment for the plaintiff employee who alleged retaliation against the prospective employer, who chose not to hire plaintiff once it learned that plaintiff had a pending Title VII action against a former employer).

(i) provide the individual with a stand-alone document clearly stating that the employer intends to procure a consumer report to be used for strictly employment purposes;

(ii) obtain the individual's written authorization for such procurement;

(iii) inform the third party that the employer has complied with the notice requirements and will not use the information to violate state or federal equal employment law;

(iv) where an adverse employment action results in part from information contained in the report, the employer must provide the individual with a copy of the relevant consumer report and a summary of the rights delineated in the FTC's "A Summary of Your Rights Under the Fair Credit Reporting Act"[338] before taking the action; and

(v) where the report is to be used for an adverse employment action, inform the individual within three business days of the decision.[339]

New York requires that the employer advise an employee or prospective employee whether a report was ordered and the name and address of the reporting agency.

4. Access to Personnel Records

Several states, including New York, have statutes that protect the personal nature of employee personnel files, and require that those accessing such personnel files do so only for a legitimate business purpose and only for a specific business transaction involving the employee. Unlike the statutes of some other states, New York's statute applies only to certain government employees, and not to the private sector. Private sector employees have no statutory entitlement to review the personnel records their employers maintain concerning them, and may review those records only if and as permitted by the employer or as provided in a collective bargaining agreement.[340]

---

338 Available at http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre35.pdf.

339 FCRA § 604(b), 15 U.S.C. § 1681b(b).

340 *See, e.g.*, N.Y. Civil Rights Law § 50-a (relating to personnel records of police and law enforcement); N.Y. Public Officers Law § 89 (relating to personnel files of public officials).

5. Polygraphs, Lie Detector Tests, and Voice Stress Analysis

The use of such equipment is limited by the Employee Polygraph Act of 1988.[341] Private employers are prohibited by the Act from requiring employees to submit to polygraphs or other lie detector tests. Public employers and certain employees involved in national defense, services for the FBI, security services, and drug manufacturing and distribution are exempt from coverage under the Act. There is also a limited exception that applies when an employer is conducting an ongoing investigation of employee misconduct involving economic loss or injury to the employer, and the employer has a reasonable suspicion that the employee was involved and had access to the property that is the subject of the investigation.

New York prohibits both public and private employers from requiring or requesting employees to submit to voice stress analysis.[342]

6. Health and Medical Data and Monitoring

Workplace issues arise in the context of employee health and medical information, and are carefully regulated, not only under the Health Insurance Portability and Accountability Act of 1996, but also under various federal and state statutes that govern matters of disability or perceived disability, family and medical leave and workers compensation, such as the Americans with Disabilities Act, the Family Medical Leave Act, the Pregnancy Disability Act, the New York Human Rights Law and the New York City Human Rights Law.

7. Race, Age, Gender, Sexual Orientation, National Origin, Religion and Other Protected Classifications

As noted in the Introduction to this Section (*see* IV. A), a number of federal and state statutes protect employees and applicants for employment from the improper use and monitoring of data in order to discriminate or retaliate against the employee or the applicant on the basis of

---

341 2929 U.S.C. § 2001 *et. seq.*

342 N.Y. Labor Law § 735.

race, age, gender, sexual orientation, national origin, religion and other protected classifications. These statutes recognize and contemplate the use of such data where pertinent to a legitimate business purpose, internal audit or other appropriate analysis or investigation to assure compliance or to permit a proper defense against allegations of discrimination or retaliation.

F. Statutory Provisions Relative To Employee Activity

1. GPS Tracking Devices by Employers

a. The use of GPS tracking devices in employees' company vehicles and phones is becoming increasingly prevalent. GPS devices can display location and movement and record both so as to establish a history the employer may access at any time. As of yet, there are no federal or state statutes that expressly prohibit the use of a GPS device in an employment situation, but state privacy statutes and common law tort principles may be sources of legal actions by employees.[343]

b. In Modesto California, a GPS tracking device was placed on a city truck used by the union's president. He filed a complaint with the state labor board alleging that in doing so, the city violated state labor laws. Although the attorney for the union president acknowledged that public employees should not expect a right to privacy while working in city vehicles, he claimed the monitoring was directed at gathering information on his union activities. Similarly, an NLRB General Counsel Advice Memorandum,[344] in agreement with the finding of the NLRB's local Regional office, advised that a non-unionized employer had violated the

---

343 *See, e.g.*, *Elgin v. St. Louis Coca-Cola Bottling Co.*, 4:05 CV 970 (E.D. Mo. Nov. 14, 2005) (during investigation of theft, employer placed GPS devices in a number of company vans employees were permitted to drive during working and non-working hours; use of the GPS tracking device was held not to constitute an actionable intrusion upon the employee's seclusion, even though he had been cleared of any wrongdoing, because "it revealed no more than highly public information as to van's location," the van was employer's property and the employer's use of the tracking device on its own vehicle [did] not rise to the level of being highly offensive to a reasonable person").

344 Case 22-CA-25324, Feb. 26, 2003.

National Labor Relations Act by interfering with employees' labor rights when it installed GPS units in the trucks of two employees who were known union organizers. The GPS units had been placed only in these two vehicles, and not in the six other vehicles in the group; the employer had constantly tracked the employees' movements even during non-working time; and the devices would have shown whether the employees went to a common location or visited the homes of other employees. The NLRB's General Counsel reasoned the employees were subjected to increased scrutiny because of their union affiliation without a legitimate business justification, in violation of the NLRA.

c. The existence of a collective bargaining agreement can change the dynamics relative to the use of GPS equipment. In *Otis Elevator Co. v. International Union of Elevator Constructors*,[345] the U.S. District Court for the Southern District of New York upheld an arbitration award in favor of the company's policy of installing GPS technology in company vehicles, noting that although the collective bargaining agreement between the employer and the union did not specifically reference the use of GPS, it granted the employer the right to use technology and to update that technology. Notably, there was no evidence of disparate treatment between known union supporters and other employees in this case, as there was in the Advice Memorandum concerning the Modesto, California employees discussed in the last paragraph above.

2. The New York Lawful Recreational Activities Law

Many states also have laws restricting employers from taking action against employees because of their private off-duty pursuits. New York State's Lawful Recreational Activities Law, Section 201-d of the Labor Law is New York's version of such laws. This statute makes it

[345] 2005 WL 2385849 (S.D.N.Y. 2005).

unlawful for an employer to discriminate against an individual because of political activities, use of legal consumable products, lawful recreational activities, or membership in a union or other union-related activities.

3. After-Hours Conduct – New York Labor Law Section 201-d

a. Section 201-d prohibits discrimination against employees for engaging in certain political and recreational activities. After vetoing two prior versions, then-Governor Cuomo considered the law in its present form to "properly strike the difficult balance between the right to privacy in relation to the non-working hours activities of individuals and the right of employer to regulate behavior which has an impact on the employee's performance or on the employer's business."

b. Political and recreational activities are defined as follows:

"Political activities" means (1) running for public office, (2) campaigning for a candidate for public office, or (3) participating in fund-raising activities for the benefit of a candidate, political party or political advocacy group;

"Recreational activities" means any lawful, leisure-time activity, for which the employee receives no compensation and which is generally engaged in for recreational purposes, including, but not limited to, sports, games, hobbies, exercise, reading and the viewing of television, movies and similar material.

c. An employer may not discharge someone, refuse to employ someone, or otherwise discriminate against someone, because of that person's: political activities outside of working hours, off of the employer's premises and without use of the employer's equipment or other property, if such activities are legal, provided, however, that this does not apply to professional journalists and newscasters (as defined in Section 79-h of the Civil

Rights Law), or federal employees;[346] Legal use of consumable products prior to the beginning or after the conclusion of the employee's work hours, and off of the employer's premises and without use of the employer's equipment or other property.

4. Smoking

The biggest battles over the right of employers to place restrictions on their employees' activities outside of working hours, and off the employer's property, were waged over restrictions on off-duty smoking. Employers felt entitled to refrain from hiring smokers, in order to maintain a healthier workforce, while critics of such policies argued that such restrictions may lead down a "slippery slope" resulting in employer attempts to exert control over any behavior that poses health risks, including consumption of alcohol, red meat, or any other substance the employer determines to be unhealthy.[347]

This debate was resolved with the passage of the New York Lawful Recreational Activities Law, which makes it unlawful for employers to discriminate against employees on the basis of an "individual's legal use of consumable products prior to the beginning or after the conclusion of the employee's work hours, and off of the employer's premises and without use of the employer's equipment or other property." Although the statute does not define "consumable products," it is widely recognized that the legislation was supported by advocates of smokers' rights.[348]

---

346 Courts have held that this prohibition applies to termination based on published allegations that subordinates were required to engage in off-duty political activity, *Melendez v. New York City Housing Auth.*, 252 A.D.2d 437 (1st Dep't 1998); and to termination based on an off-duty political argument with a supervisor, *Cavanaugh v. Doherty*, 243 A.D.2d 92 (3d Dep't 1998); and to denial of promotion and compensation based on employee's off-duty political activities, *Richardson v. City of Saratoga Springs*, 246 A.D. 2d 900 (3d Dep't 1998).

347 See Brendan W. Miller, Your Money Or Your Lifestyle!: Employers' Efforts To Contain Healthcare Costs: Lifestyle Discrimination Against Dependents of Employees, 5 Ind. Health L. Rev. 371, 385 (2008).

348 Memorandum of William J. Pellegrini, Governor's Office of Employee Relations (July 14, 1992).

Although the Lawful Recreational Activities Law prohibits discrimination because of an employee's off-duty and off-premises conduct, it does, however, permit an employer to require an employee to bear the cost of higher premiums for health, life or disability insurance on the basis of their use of tobacco or other lawful, yet unhealthy, products.[349]

5. Dating

New York intermediate appellate courts consistently have held that "dating" a co-worker is not a protected activity under 201-d, as it is "entirely distinct from and bears little resemblance to a recreational activity." Accordingly, workplace policies prohibiting fraternization between co-workers have been upheld as lawful and not in violation of the Lawful Recreational Activities Law.[350] The Court of Appeals has not yet opined on this subject.

These cases also stand for the proposition that an employer's prohibition of co-workers from engaging in romantic relationships is a valid business interest. *See* N.Y. LAB. LAW Section 201d, which expressly exempts from protection conduct by employees that "creates a material conflict of interest related to the employer's trade secrets, proprietary information or other proprietary or business interest." Specifically, it is believed that relationships among co-workers can result in decreased productivity in the workplace and potential claims of workplace sexual harassment or discrimination, and hence fall within this exemption.

It must be noted that while courts have been willing to uphold policies that bar relationships between co-workers as lawful under the Lawful Recreational Activities Law, the

---

349 N.Y. LAB. LAW § 201-d(6).

350 *See State of New York v. Walmart Stores, Inc.*, 207 A.D. 2d 150 (3d Dep't 1995), where the Court held the retailer did not violate Section 201-d when it discharged two employees for violating a no fraternization policy which prohibited a "dating relationship" between a married employee and another employee, other than his or her spouse; *See Hudson v. Goldman Sachs & Co., Inc.*, 283 A.D.2d 246 (1st Dept. 2001) (romantic relationships are not protected "recreational activities" within the meaning of that provision; *McCavitt v. Swiss Reinsurance Am. Corp.*, 237 F.3d 166, 168 (2d Cir. 2000) (employer termination of employees who violated the non-fraternization policy lawful).

lines have been drawn between co-worker relationships and relationships occurring outside of the workplace.[351]

a. Section 201-d also prohibits discrimination based on "an individual's membership in a union or any exercise of rights granted under [the National Labor Relations Act] or under [the Taylor Law]." It has been held that this provision protects individuals who belong to a union that is not covered by the National Labor Relations Act or the Taylor Law (*e.g.*, parochial school teachers).[352]

b. These prohibitions do not apply to a person with whom an employer has a professional service contract, and "the unique nature of the services provided is such that the employer shall be permitted, as part of such professional service contract, to limit the off-duty activities which may be engaged in by such individual."

c. An employee's activity is not protected if that activity:

(i) creates a material conflict of interest related to the employer's trade secrets, proprietary information or other proprietary or business interest;

(ii) knowingly violates statutory or contractual conflict of interest provisions applicable to state and local government employees; or

---

351 For example, in *Pasch v. Katz Media Corp.*, No. 94 Civ. 8554 (RPP), 1995 U.S. Dist. LEXIS 11153 (August 4, 1995), the plaintiff claimed that she was discriminated against in violation of 201-d because she was fired for cohabitating with a former company employee allegedly "outside work hours, off the employer's premises". *Id*. at 5. In declining to dismiss the Complaint, the court held that "a careful reading of the statute and its Pocket Bill indicates that "cohabitation that occurs off the employer's premises, without use of the employer's equipment and not on the employer's time, should be considered a protected activity for which an employer may not discriminate, absent some showing that such activity involves a material conflict of interest with the employer's business interests. *Id*. Similarly, in *Aquilone v. Republic Natl. Bank of N.Y.*, 98 Civ. 5451 (SAS), 1998 U.S. Dist. LEXIS 19531 (S.D.N.Y., December 14, 1998), the court found that allegations that the plaintiff was discharged because of an out-of-work friendship was sufficient to support a claim under N.Y. Labor Law §201-d.

352 Muhitch v. St. Gregory the Great Roman Catholic Church and School, 239 A.D.2d 901 (4th Dep't 1997).

(iii) violates a collective bargaining agreement or a contract entered into by a certified or licensed professional, provided the person's annual compensation is equivalent to at least $50,000 in 1992 dollars.

(iv) An employer may also avoid liability by showing that it took action based on the belief that:

(a) the employer's actions were required by statute, regulations, ordinance or other governmental mandate;

(b) the employer's actions were permissible pursuant to an established substance abuse or alcohol program or workplace policy, professional contract or collective bargaining agreement; or

(c) the individual's actions were deemed by an employer or previous employer to be illegal or to constitute habitually poor performance, incompetency or misconduct.

(v) An employer may charge different premiums for health, disability, and life insurance based on behaviors (such as smoking) if the differential reflects actual cost to the employer, and employees are provided with a statement of the differential rates charged by the carrier.

(vi) Enforcement of Section 201-d may be by the attorney general, or by an "aggrieved individual":

(a) courts may impose a civil penalty of $300 for the first offense and $500 for each subsequent offense; and

(b) an individual may receive equitable relief and damages.

6. <u>New York State Workplace Violence Prevention Act</u>

This law, codified under New York Labor Sec. 27-b, became effective October 5, 2006 and requires public employers to evaluate safety and health hazards in the workplace and implement employee protection programs. Under the Act the following is required:

- Every public employer must evaluate the workplace to determine any factors that might place employees at risk of assault or homicide, including public settings, late night or early morning hours, the exchange of money with the public, uncontrolled access to the workplace and areas of previous security problems.

- Every public employer with at least 20 permanent full-time employees must develop and implement a written workplace violence prevention program which includes a list of risk factors present in the workplace and the methods the employer will adopt to prevent violent

incidents, including making high-risk areas more visible, installing good lighting, reducing the presence of cash, training in conflict resolution and self-defense and establishing a report system for incidents of aggression.

- A public employer with at least 20 permanent full-time employees must make the written violence prevention program available, at request, to its employees, their designated representative and the department;

- Every public employer must provide its employees with the following information and training at the time of their initial assignment and annually thereafter: information on the requirements of the Workplace Violence Prevention Program, the risk factors in the workplace, and the availability of the workplace violence prevention program; and training that includes at least: the measures employee can take to protect themselves, including specific procedures implemented by the employer, such as appropriate work practices, emergency procedures, use of security alarms and other devices and the details of the written workplace violence prevention program.

In the application of such programs, where an employee believes there is a serious violation of the protection program or an imminent danger exists, he or she must bring the matter to the attention of a supervisor, in writing. If after a reasonable opportunity the employer does not resolve the problem and the employee still believes a violation of the prevention program remains or that an imminent danger still exists, the employee may request an inspection by giving notice to the commissioner in writing. The inspection shall be made forthwith and the commissioner must supply a copy of the notice to the employer prior to the inspection. The employee giving the notice may request his or her name be withheld.

At the inspection, a representative of the employer and an authorized employee representative have the opportunity to accompany the commissioner. The commissioner is not limited to the alleged violation and may inspect any other area of the premises in which he or she has reason to believe a serious violation exists. The commissioner, on his or her own initiative, can conduct an inspection of any premises if reason to believe a violation of this section has occurred or a general schedule of inspections.

No retaliatory action can be taken by the employer against any employee because the

employee:

- Gives written notice to the employer regarding belief a serious violation of the violence protection program exists or there is imminent danger;
- Requests an inspection by giving notice to the commissioner;
- Accompanies the commissioner during his or her inspection.

G. Statutory Provisions Relative to Use of Employer Systems

1. National Labor Relations Act (NLRA) Considerations

a. Non-discrimination Rules

Under NLRB law, if the employer allows its employees to use its e-mail system for personal reasons, it may not prohibit use of the e-mail system by employees for union activity, such as to confer about whether or not to join a union.[353]

b. Prohibitions On All Non-Business Use?

Unions use the Internet as an organizing tool by contacting employees directly through e-mail. In addition, many unions have their own web sites that employees may visit from workstation computers.

In *The Guard Publishing Co., dba The Register Guard,*[354] the National Labor Relations Board held that an employer with an established rule prohibiting the use of the employer's e-mail system for non-job-related solicitations did not violate Section 8(a)(1) of the NLRA when it applied this rule to bar employee efforts to solicit support for a union. The Board majority determined that the employer's e-mail system is company property and employees have no statutory right to its use. Although in this case, the employer had permitted *personal* e-mail

353 *See E.I. DuPont de Nemours & Co.,* 311 NLRB 893 (1993). The Courts of Appeals have not fully embraced the Board's discrimination theory in this regard (*see, e.g., Salmon Run Shopping Center v. NLRB,* 534 F.3d 108 (2d Cir. 2007); *Sandusky Mall Co. v. NLRB,* 242 F.3d 682, 686-87 (6th Cir. 2001)), so it remains an unsettled question whether it necessarily follows from the fact that an employer permits use of its e-mail system for personal reasons that the employer would be required to permit use of that same e-mail system for union activity.

354 *The Guard Publishing Co., dba The Register Guard,* 351 NLRB No. 70 (2007); *see* General Counsel Ronald Meisburg's Memorandum at GC 08-07.

solicitation, the employer had not permitted e-mails soliciting support for an *outside* group or organization. The Board viewed the union as an outside organization and held that the employer had lawfully enforced its policy against two employee e-mails that had solicited support for the union.

On May 15, 2008, the General Counsel of the Board issued a memorandum that reports on case developments involving the *Register Guard* decision and the following five cases:

- An employer's rule barring union officials from sending e-mails to company managers outside of the facility was found to be lawful. The employer previously had allowed the union to use the company's e-mail system to conduct union business and to communicate with the employer about labor relation matters at the facility. Here, however, the union was using the company's e-mail system to send broadly distributed e-mails to company managers outside the facility. The General Counsel found the rule to be lawful because it concerned how the union was permitted to use the employer's e-mail system and did not otherwise prohibit the union from engaging in protected communications outside the plant or to broad groups of manages. Since the rule solely involved company equipment, and did not discriminate against union or other activity protected by Section 7 of the NLRA, it was considered lawful.

- A health care facility employer maintained a no-solicitation rule which, on its face, prohibited solicitation for any purpose during working time and in immediate patient care areas. However, this rule, it was found, had been applied inconsistently – the employer warned and disciplined employees who engaged in union solicitation activity, and yet allowed non-union related solicitation for commercial and individual activities school fund-raising campaigns and personal reasons. The General Counsel reasoned that an employer may not discriminatorily enforce a facially valid no e-mail solicitation rule.

- An employee sent e-mails to about 20 co-workers about an off-site union organizing meeting. Prior to sending the e-mails, the employee consulted with the IT Director as to what was considered an abuse of the employer's e-mail system. The IT Director did not inform the employee that personal e-mail or e-mail solicitation was against employer policy. After sending the e-mail communication about the union meeting, the employee received a written warning for using the e-mail system for solicitation purposes in violation of handbook provisions. However, evidence established that supervisors and other employees frequently sent non-work related e-mails at work and during working times. The General Counsel concluded the employer re-promulgated its e-mail rule for anti-union reasons, and discriminately enforced the rule against union activity.

- Another employer was found to have discriminatorily enforced its electronic communications policy. An employee, acting on behalf of a group of employees, sent e-mails to the employer's Board of Directors and House of Delegates seeking assistance in presenting a petition on working conditions. When the identity of the e-mail author was discovered, his employment was terminated because the employer claimed he had used its e-mail system

improperly and disrupted operations. The employer was found to have fired the employee unlawfully, because the employer's e-mail policy allowed reasonable personal use of the employer's computer and the employer permitted extensive use of the Internet, e-mail and other company equipment for personal purposes. In this case the employer had enforced its e-mail policy disparately against protected concerted activity.

- Employer discriminatorily applied its unwritten bulletin board policy. At the time of union organizing activity, employer maintained two bulletin boards: one was used for official announcements and the other was used by employees for all types of personal or general non-work related matters. A union supporter posted on the employee bulletin board a list of union demands and a union leaflet. The letter and leaflet were removed, yet other personal announcements remained. Eventually all employee postings were removed and replaced by employer materials. The General Counsel found the abrupt change in activities evinced an anti-union motivation.

c. Solicitation? Distribution?

Application of the NLRB's traditional solicitation/distribution rules to the world of email and other electronic communications media has tended to focus the analysis on the nature of the communication at issue – is the e-mail a "solicitation" which may be banned entirely? Or is it "distribution" activity, which may not be prohibited in non-work areas during non-work time? Are some e-mails properly labeled as "solicitations" and others labeled properly as "distributions"?

d. The Equipment

The Board's long-standing employer equipment rules (which generally evolved from cases in which telephones constituted the employer equipment at issue) ask first, and regardless of the nature of the communication, whether the employee is using employer equipment to effect the communication. If so, the employee has no presumptive right to use employer property.

e. Mandatory or Non-mandatory Subject of Bargaining

To date, the NLRB has not ruled on whether Internet and e-mail access and monitoring are mandatory subjects of bargaining that unions may demand that employers bargain over. One argument as to why employer monitoring of e-mail and Internet use may be a mandatory subject

of bargaining would be based on the theory that such monitoring implicates employee discipline, which has been held to be a term and condition of employment.[355]

H. Blogging – The Rights and Obligations of Employers and Employees

In general, employers maintain that they have no obligation to hire or continue the employment of someone who publishes a "web log" (or a "blog") that disparages the employer or the employer's products or personnel, that subjects the employer to unwanted publicity, that discloses the employer's confidential information, that contributes to unlawful harassment of co-workers of the blogger, or that might otherwise cause legal, business, or competitive harm to the employer. Employees generally maintain that they have an unfettered right to publish whatever they wish to publish on the Internet, without "snooping" from or interference by the employer; many also assert that they have the right to say whatever is on their mind anonymously, and that it is an unwarranted invasion of their privacy for employers to interfere with blogging activities, particularly where the employee engages in them before or after work, wholly removed from the employer's premises.

Little case law has yet been developed in New York, or elsewhere in the country, which addresses employer policies that regulate employee blogging activity, suggesting that there may well be no problem that needs to be fixed in the area of employer regulation of employee blogging activities. However, there is anecdotal evidence that some employers have fired some employees because of the content of their blogs.[356] Indeed, the "blogosphere" has coined a phrase – getting "Dooced" – that refers to an employee's being discharged for statements made

---

355 *Cf. Colgate-Palmolive Co. v. Local 15, International Chemical Workers Union*, 323 NLRB No. 82 (1997) (company's installation and use of workplace surveillance cameras constituted a mandatory subject of bargaining due to impact on the disciplinary process).

356 *See* Pamela A. MacLean, *Employers Winning Blog Suits – So Far*, NAT'L L.J., Jan. 26, 2007, available at http://www.law.com/jsp/article.jsp?id=1169719347007.

on the employee's blog.[357] So we will address the issue here.

In New York, which has no law that limits an employer's right to discipline an employee for what the employee says on a blog, an employer generally is free to discipline or discharge an employee for his or her blogging activity. However, there are a number of statutory and common law restrictions that might limit an employer's otherwise unfettered right to terminate employment because of statements made on an employee's blog, such as New York State's Lawful Recreational Activities Law and whistleblower statutes, the NLRA, and other federal laws.

1. The New York Lawful Recreational Activities Law

Although New York courts have not yet applied the protections of N.Y. Labor Law Section 201-d to blogging, the fundamental protections of the law (*i.e.*, prohibiting discrimination due to lawful recreational activity) extend to blogging, especially if the subject matter of the blog is not related to the workplace or the blogger's employment.

However, if the employee blogs about his or her workplace, especially in a manner that is detrimental to the employer's business, the New York Lawful Recreational Activities Law may well afford no protection at all. The statute does not protect activity which "creates a material conflict of interest related to the employer's trade secrets, proprietary information or other proprietary or business interest."[358] While it is not clear how broadly the courts will interpret the phrase "other…business interest," employers most likely would attempt to rely on the "business interest" provision in an effort to protect the employer's reputation, corporate image and trade secrets. . As yet there have been no blogging cases litigated under this statute, and the parameters of the statutory definition "recreational activities" are far from sufficiently settled to

---

357 Heather Armstrong, a web designer, was fired in 2001 for writing "objectionable and negative" statements about her job, co-workers and boss on her blog, Dooce.

358 N.Y. LAB. LAW § 210-d(3)(a).

predict where the limits of employee conduct and employer regulation in the area of blogging eventually will be drawn.

2. New York's Whistleblower Law

New York's whistle-blower statute prevents any retaliatory personnel action against an employee who "discloses…an activity, policy or practice of the employer that is in violation of law, rule or regulation which…creates and presents a substantial and specific danger to the public health or safety."[359] This statute may provide some protection to bloggers who discuss issues connected with public health or safety. However, to trigger the protection of the law, the employee must complain about an actual violation that creates a substantial and specific danger to public health and safety. Complaining about a belief that a violation has occurred is not enough to trigger the protection of the statute.[360]

3. National Labor Relations Act

The content of an employee's blog may be considered "concerted activity" and, as such, subject to the protection of Section 7 of the National Labor Relations Act ("NLRA")[361] and the New York Labor Law, which creates a system similar to the NLRA. Although New York courts have not addressed the issue of blogging in the context of the NLRA, a Michigan Court of Appeals recently upheld a Michigan Employment Relations Council decision that a police officer was wrongfully suspended for maintaining a personal blog that criticized the police chief.[362] The case was decided under Michigan's Public Employment Relations Act ("PERA"), which uses

---

359 N.Y. LAB. LAW §740(2)(a). Retaliatory action by public employers is covered at Civil Service Law § 75-b.

360 *See Calabro v. Nassau Univ. Med. Ctr.*, 424 F.Supp.2d 465, 475 (E.D.N.Y. 2006).

361 The NLRA applies to union and non-union employees. An employee fired for blog or chatroom posting can file an unfair labor practice charge under the NLRA, and, if those postings are determined to be protected concerted activities, be reinstated with back pay.

362 See City of Detroit v. Detroit Police Officers Ass'n, 2007 WL 4248562 (Mich. App.).

language modeled on that of the NLRA in identifying what activity is protected.[363] The Court held that the officer, although acting alone, operated at least part of the web site to induce group activity for the mutual aid and protection of fellow police officers, and, therefore, his activity was protected under PERA.

Similarly, in *Valley Hosp. Med. Ctr. v. Nevada Serv. Employees Union*,[364] an intensive care nurse employed at a Nevada hospital, who served as a union representative for her RN unit, was discharged after she publicized concerns that nurses had brought forward during contract negotiations. In addition to being quoted in the print media about staffing shortages in the intensive care unit, the nurse posted to a non-union message board. Her write-up described staffing situations that occurred, suggested possible impacts on the patients, and opined that the hospital could afford to bring on more staff but had chosen not to. The NLRB found that both the print story and the web posting constituted protected discourse because they touched on the collective bargaining controversy and staffing issues.

However, the NLRA does not protect all employee speech, and employees who engage in disloyal behavior or who disparage the employer's customers or business activities will not necessarily be protected by the Act.[365] A key concern for the Board in analyzing claims of violations of the NLRA in this context is whether the employee solicited fellow employees for union-related purposes, though a claim based on mutual aid and protection may also be successful as long as employees other than the blogger are visiting the web site (or, perhaps, even if no other employees visited the web site, as long as the blogger entertained a reasonable belief that they would read it).

---

363 Section 9 of the Act says that "[i]t shall be lawful for public employees to…engage in lawful concerted activities for the purpose of collective negotiation or bargaining or other mutual aid and protection…"

364 Valley Hosp. Med. Ctr. v. Nevada Serv. Employees Union, 2007 NLRB LEXIS 192.

365 See NLRB v. Local Union No. 1229, I.B.E.W., 346 U.S. 464, 477-78 (1953).

4. Other Federal Provisions

It is well-established that First Amendment rights, for the most part, do not extend to employees in the private sector.[366] No court has been asked to address what limits First Amendment protections place on public-sector employers' ability to discipline workers for blogging activity. Similarly, courts have not considered whether blogging is "protected activity" subject to Title VII of the Civil Rights Act of 1964's anti-retaliation provisions. However, courts have held that informal protests of discriminatory employment practices are protected, thereby suggesting that such protests contained in a blog might well be considered "protected activity" under Title VII for which an employer could not lawfully retaliate against the blogger/employee.[367]

The whistleblower provisions of the Sarbanes-Oxley Act of 2002 ("SOX") may also provide protection for an employee's blogging activities. SOX protects employees of publicly traded companies who report, among other things, allegations of financial improprieties or laws, rules or regulations relating to fraud against shareholders. To invoke the SOX whistleblower protection, the employee is required to first report the unlawful conduct to a supervisor, a federal regulatory or law enforcement agency, or a member of Congress.[368] Nevertheless, unless an employee complained to his or her supervisor, a federal regulatory or law enforcement agency, or a member of Congress, it appears that a publicly traded company may lawfully terminate an employee for blog entries related to alleged financial improprieties.

Federal and state anti-discrimination laws also may provide rights to the employee blogger (or, at the very least, provide grounds for legal action against the employer). Given the

366 *See Engstrom v. Kinney Sys., Inc.*, 241 A.D.2d 420, 422 (1st Dept. 1997) (finding that dress code requirements did not infringe on employee's religious practices).

367 *Summer v. United States Postal Serv.*, 899 F.2d 203, 209 (2d Cir. 1990).

368 18 U.S.C. § 1514A.

right set of facts, a blogger might claim that he or she was treated differently from co-workers who engaged in similar activity because of sex, race, national origin, age, etc. (as demonstrated by the lawsuit brought by Ellen Simonetti against Delta Airlines after she was discharged for her blog's content). An employee blogger who discusses his or her previously unknown sexual orientation, or religion, may claim that their discharge was a pretext for discrimination on the basis of that previously undisclosed protected characteristic.

5. Proposed Model Statute

A recent law review article[369] presented a proposed model statute to define and protect lawful blogging activity. The proposed statute reads as follows:

> (1) It shall be a discriminatory or unfair employment practice for any employer to refuse to hire an applicant, demote, or to terminate the employment of any employee, or to fail or refuse to promote or upgrade an employee, due to that applicant's or employee's engaging in any lawful activity or conduct or speech associated with the protected activity or conduct when done off the premises of the employer during nonworking hours unless such a restriction:
>
> (a) Relates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee or a particular group of employees, rather than to all employees of the employer; or
>
> (b) Is necessary to avoid a *bona fide* and actual conflict of interest with any responsibilities of the employer or the appearance of such a conflict of interest.

I. First Amendment Associational Rights

In a 2007 decision, the Second Circuit upheld the discharge of several corrections officers whose employment had been terminated because they were members of the Connecticut chapter of the Outlaws motorcycle gang.[370] The Department of Corrections' regulations prohibit employees from engaging in "unprofessional or illegal behavior, both on and off duty, which

---

369 Untangling the World Wide Weblog: A Proposal for Blogging, Employment at Will, and Lifestyle Discrimination Statutes, 42 Val. U.L. Rev. 245, 276 (2007).

370 *Piscottano v. Murphy*, 511 F.2d 247 (2nd Cir. 2007).

could in any manner reflect negatively on the Department of Correction."[371] The Court held that the employer's "policy" was specific and rejected the employees' claims that the terminations of their employment violated the First Amendment to the United States Constitution's freedom of association.[372] The Court held that because several other state chapters of the Outlaws had been prosecuted for racketeering and other felonies, membership in the gang had the potential to disrupt and undermine the Department's operations.[373]

371 *Id*. at 256.
372 *Id*. at 268 and 280–82.
373 *Id*. at 276-77.

V. FEDERAL STATUTES AND REGULATIONS THAT IMPOSE A DUTY ON FINANCIAL BUSINESSES WITH REGARD TO THE COLLECTION, SHARING AND SAFEGUARDING OF CUSTOMER INFORMATION

The federal government and the states have enacted laws and regulations requiring banks, creditors, retailers and other businesses to safeguard the customer data entrusted to them and to use care in the disposal of records which contain such information. It is the states, however, which have actively imposed laws with respect to security breaches – requiring a business entity (and in some cases the government agency) to advise its customers that their private personal information may have been compromised due to an unauthorized access of the computer network of the business, a lost laptop containing customer information and, in certain states, wrongful access or use of personal information, and in certain states, wrongful access or use of personal information contained in paper files. These state laws typically require the business to notify their customers of what steps they should take to guard against identity theft.

A. Gramm-Leach-Bliley: a Federal Standard for Consumer Privacy

1. Overview and Introduction

The Gramm-Leach-Bliley Act of 1999 ("GLB")[374] established a federal standard of privacy that protects individuals in their dealings with entities that provide financial services and products for personal, family or household purposes. These purposes are sometimes referred to as "consumer purposes."

The GLB imposes on each financial institution an "affirmative and continuing obligation" to respect the privacy of its customers. The GLB limits the instances in which a "financial institution" may disclose non-public personal information about a consumer to nonaffiliated third parties. It requires financial institutions to have a written privacy policy that describes what that entity may do with the customer's non-public personal information that it has

[374] Pub. L. 106-102, 113 Stat. 1338.

collected. GLB requires that this policy be disclosed at the time that a customer relationship is established and that it be updated annually. Subtitle A of GLB also requires that the administrative agencies regulating financial institutions develop standards relating to the administrative, technical and physical safeguards that financial institutions need to adopt to insure the integrity of customer data and to protect that data against anticipated threats or unauthorized access.[375]

The privacy provisions of GLB are limited to consumer transactions with financial institutions. Under GLB, a "consumer" is defined as an individual who obtains financial products or services from a financial institution which are to be used primarily for personal, family or household purposes. The GLB also defines "consumer" to include a representative of that individual.[376]

GLB further protects financial institution customers by prohibiting any person or entity from obtaining non-public personal information on a customer of a financial institution on a false or fraudulent basis.[377] Intentional violations of this provision are subject to criminal penalties including fines and imprisonment.[378]

The term "financial institution" is defined in GLB to mean, in general, any institution whose business is engaging in "financial activities" as described in section 4(k) of the Bank Holding Company Act of 1956.[379] The list of "financial activities" is quite extensive – the GLB applies to virtually any business that provides (or offers to provide) any financial product or service to a consumer, including depository institutions (*e.g.*, banks, thrifts, credit unions), any

375 15 U.S.C. § 6801(a) (GLB, Subtitle A of Title V, entitled "Disclosure of Non-Public Personal Information").
376 15 U.S.C. § 6809(9).
377 GLB, Subtitle B, Title V, entitled "Fraudulent Access to Financial Information."
378 16 USC § 6823.
379 15 USC § 6809 (3).

broker or dealer (as defined under the Securities Exchange Act of 1934), investment advisor, investment company, insurance company, loan or finance company, loan broker, consumer reporting agency, and credit card issuer.[380] It also applies to entities like auto dealers that arrange financing for consumers and retail stores that establish credit accounts or store credit cards, even if the cards are issued by another entity.

Enforcement of this federal privacy statute is delegated to the federal regulators or other authority governing each particular type of financial institution.[381] For example, the federal banking agencies are the privacy regulator for banks under their supervision; securities brokers or dealers and investment companies are subject to the authority of the Securities Exchange Commission ("SEC"); and insurance companies are subject to the applicable State insurance authority where they are located. The FTC is the "catch-all" regulator for any other financial institution or person that is not supervised by one of the agencies identified in GLB, such as most non-bank creditors and loan brokers whose primary regulator is not the SEC, including sales finance companies, creditors which finance the sale of products or services like car dealers, mortgage brokers, finance companies and similar entities.

The GLB directs each government agency or authority that regulates a financial institution to issue implementing regulations.[382] The balance of this Section will focus on the joint privacy regulations issued by the federal banking agencies: 12 C.F.R. Part 40 (Office of the Comptroller of the Currency ("OCC"); 12 C.F.R. Part 216 (Federal Reserve System ("Fed")); 12 C.F.R. Part 332 (Federal Deposit Insurance Corporation ("FDIC")); and 12 C.F.R. Part 573 (Office of Thrift Supervision ("OTS")).[383] As many of these regulations are substantively

---

380 Bank Holding Company Act of 1956, Section 4(k).

381 15 USC § 6805.

382 15 USC § 6804.

383 Note that the National Credit Union Administration ("NCUA") has its own privacy regulations at

identical, the focus of this Report will be on the privacy regulations issued by the Federal Reserve, sometimes known as "Regulation P".[384]

2. Privacy Policy-Timing & Contents

The privacy regulations state that a financial institution primarily owes a duty to protect the personal information of a consumer that is its customer. Under these regulations, the financial institution must provide a copy of its privacy policy to the consumer not later than the time when a customer relationship is created. The regulations provide some examples of "when" a customer relationship is established, such as when a customer opens a credit card account, executes a contract to open a deposit account, purchases insurance, obtains credit, becomes a client for purposes of the provision of credit counseling or tax preparation services, or agrees to obtain some financial service in exchange for a fee.[385]

With respect to loans, the same regulations provide that a financial institution establishes a customer relationship with a consumer who obtains a loan for personal, family or household reasons at the time the entity originates the loan or at the time the entity purchases the servicing rights to the consumer's loan.[386]

A hypothetical example illustrates the application of these rules. A consumer who uses a mortgage broker to assist in obtaining a residential mortgage loan will receive a privacy notice from the mortgage broker at the time that the consumer becomes a customer of the mortgage broker.[387] When the customer finds a lender, that lender will provide a copy of its privacy notice to the customer. If, subsequent to the closing, that loan is sold to another entity, and an entity other than the original lender services the loan, the servicer is required to issue its privacy notice

---

12 C.F.R. Part 716.

384 12 C.F.R. Part 216. For the full text of the FTC regulations see 16 C.F.R. Part 316 and SEC (17 C.F.R. Part 248).

385 12 C.F.R § 216.4

386 12 C.F.R. § 216.4.

387 16 C.F.R. Part 313.

to the consumer as it will be sending the billing statements, accepting payments and otherwise dealing with the consumer while the loan is being repaid.[388]

The initial privacy notice is intended to give the customer advance information about what a financial institution may do with any non-public information about the customer that it collects. This applies to information that is provided to the entity in the course of the individual consumer becoming, or in remaining, a customer (*e.g.,* Social Security number, employment information, other sources of income, information on savings/assets, types and frequency of transactions, etc.).[389] Except under limited circumstances, if the company's policy reserves the right to share that non-public personal information with non-affiliates, it must offer the consumer the right to "opt-out" of such sharing and describe the methods by which the consumer can exercise that right so that the non-public personal information will not be shared.[390] Companies can also share non-public credit information in their possession about their customers with their affiliates (*e.g.,* information obtained from a consumer report or an application such as income and assets) <u>if</u> they offer consumers the same right to "opt out" before doing so.[391] Once selected, each of these "opt-out" elections remain in effect until revoked by the consumer.

Business entities must also disclose if they reserve the right to share non-public personal information of a consumer with non-affiliated third parties to assist that entity in marketing its

---

388 12 C.F.R. Part 216.4 (c) (2).

389 12 C.F.R. § 216.6(a).

390 12 C.F.R. § 216.6(a)(6).

391 12 C.F.R. § 216.6(a)(7), referencing FCRA § 603(d) (2) (A) (iii), codified at 15 USC § 1681a(d)(2)(A)(iii).) Under the law, financial institutions are generally permitted to share transaction or experience information on their customers with credit reporting agencies and other potential creditors/insurers having a legitimate need for the information – so this right of "opt-out" is limited to the sharing of "other information" such as the information on a credit application including income level, assets, liabilities, etc. The FTC has stated that if a financial institution's information sharing is subject to a consumer's right to opt out, the financial institution must wait a reasonable period of time (30 days from delivery of its privacy notice is generally considered sufficient) before sharing information so the consumer has time to consider whether to opt out at the beginning of the relationship. 16 C.F.R. § 310.10. Also, *see* the Reuse and Redisclosure prohibitions at 16 C.F.R. § 313.11.

own products or services or for a joint marketing effort between the financial entity and a third party.[392] No customer right of opt-out applies to this type of information sharing. Note, however, that the regulation also provides that in any joint marketing arrangement, the third party can only use the non-public personal information to assist the entity in marketing its products or within the confines of the joint marketing program. That third party may not independently use any of that "shared" information for its own independent purposes.

In addition, entities must disclose if they reserve the right to share customer information with third parties to service or process transactions at the consumer's request, or which are otherwise necessary to provide the service. For example: sharing non-public information about transactions/payments with a third party in a private label credit card offered jointly by a bank and a third party or advising a merchant whether there is sufficient balance in a deposit account to cover a check the consumer is presenting to the merchant for a purchase, etc.[393] The financial institution must also advise that the non-public information will be shared with third parties as required by law, *e.g.*, such as when the entity is served with a subpoena requesting information about customer records, or when the entity is required to provide its transaction experience with credit reporting agencies under the Fair Credit Reporting Act.[394] Again, the customer has no right to 'opt-out' of these types of information sharing.

The privacy notice must also indicate how the financial institution treats the non-public information of former customers[395] and the entity's policies and procedures with respect to protecting the security and confidentiality of information it has obtained.[396]

Each financial institution is also required to send a copy of its current privacy policy to

---

392 12 C.F.R. § 216.13.
393 12 C.F.R. § 216.14.
394 12 C.F.R. § 216.15.
395 12 C.F.R. § 216.6(a)(4).
396 12 C.F.R. § 216.6(a)(8).

all its consumer customers on an annual basis thereafter.[397]

3. Safeguards Rule and Consumer Information Disposal Rule

The GLB also requires each federal agency or other governmental authority regulating a financial institution to establish standards to protect the security and confidentiality of financial institution customer records and information, to protect against any anticipated threats or hazards to the security or integrity of those records, and to protect against unauthorized access to or use of those records.[398]

The federal banking agencies and the Federal Trade Commission adopted "Interagency Guidelines Establishing Standards for Safeguarding Customer Information,"[399] which sets forth standards pursuant to sections 501 and 505 of the GLB[400] called the "Safeguards Rule".[401] The Safeguards Rule requirements govern the developing and implementing of administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. They also address standards with respect to the proper disposal of consumer information, pursuant to sections 621 and 628 of the Fair Credit Reporting Act.[402]

"Consumer information" in the context of a bank agency or financial institution "Safeguards Rule" is defined as follows:

> any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the bank or financial institution for a business purpose. Consumer information also means a compilation of such records.

397 12 C.F.R. § 216.8.
398 15 U.S.C. § 6801(b)(1)–(3).
399 12 C.F.R. Part 30, App. B-OCC; 12 C.F.R. Part 208, App. D-2 – Fed & Part 225, App. F-Fed; 12 CRF Part 364, App. B – FDIC; and 12 C.F.R. Part 570, App. B-OTS.
400 15 U.S.C. § 6801 and 6805.
401 12 C.F.R. Part 208, App.D-2.
402 15 U.S.C. §§ 1681s and 1681w. For other regulations *see* 16 C.F.R. Part 314 – FTC; 17 C.F.R. 248- SEC.

> The term does not include any record that does not identify an individual.[403]

Under the Safeguards Rule, a "bank or financial institution" must implement a comprehensive written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the bank or financial institution. A bank or financial institution must ensure that all elements of the information security program are coordinated, although different departments of a bank or financial institution may not necessarily have identical policies and procedures. A bank or financial institution is responsible for ensuring that its subsidiaries also implement a comprehensive information security plan. The Board of Directors or a committee that it designates must approve the bank's or financial institution's written plan and oversee the development and maintenance of it.

The Safeguards Rule recognizes that each bank or financial institution may approach this task differently, but the written plan must, at a minimum, address each of the items identified in the Safeguards Rule including: a statement of program objectives, identification and assessment of the risk of the threat of the loss, theft or misuse of personal customer data; and development of a program designed to manage and control such risks, including the imposition of access restrictions at physical locations containing customer information, encryption of electronic customer information, employee background checks, and similar protective measures.

The plan must provide for staff training, a regular program to test the controls in place, and the proper disposal of customer records. It must also address the use of third-party service providers which are required to adopt similar data and personnel security provisions designed to protect the unauthorized use or loss of any customer data provided to them by the bank or financial institution. Finally, the plan must also set forth a response program that a bank or

---

[403] 12 C.F.R. 208 App. D-2 (C) (2) (b.)

financial institution is to follow when it suspects or detects that unauthorized individuals have gained access to customer information systems. This "Response Program" is discussed in greater detail herein (*See* Section V.F.) in the context of "Identity Theft".

As noted above, Title V of GLB and the implementing regulations are subject to enforcement by the functional regulator of the financial institutions, although the GLB does not specifically provide for a private right of action.[404] If the financial institutions' actions were deemed to be "deceptive," the customer or a State official such as an Attorney General may also consider pursuing a private action under applicable "deceptive practice" laws. Many state deceptive practice laws deem violations of federal consumer protection laws or regulations to be violations of these state laws as well.

B. Fair Credit Reporting Act, Including Amendments by the 2003 Fair and Accurate Credit Transactions Act "FACTA"

1. Credit Reports

The Fair Credit Reporting Act[405] ("FCRA") was initially enacted to protect information collected by consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services. The primary regulator that enforces violations of FCRA is the FTC.[406]

---

404 Whether the GLB should provide for a private right of action, and why the existing statute does not provide for such a private action, is worthy of further study. All of the federal banking agencies provide a general administrative procedure for anyone to contact them and submit a written complaint about a bank to which the bank is permitted to respond. The Federal Reserve web site provides a link to the bank and financial service regulators and how to file a complaint. http://federalreserve.gov/consumerinfo/agency.htm; *See also* http://www.occ.treas.gov/customer.htm. However, it is not clear that complaints to regulators result in meaningful consumer remediation and any actions are not publicized. Historically, regulators address these issues globally in compliance or other examinations as a part of their general supervisory work. Neither the results of these examinations nor any remediation actions taken by the regulators are publicized. Agency regulation of financial institutions' compliance practice is done largely through compliance and other examinations as part of their general supervisory activities and the results are not made public.

405 15 U.S.C. §§ 1681-1681(x).

406 Other agencies are authorized to enforce compliance with FCRA by the entities which they

Under the FCRA, individuals have the right to receive at no cost one copy of his or her credit report from each of the three national credit bureaus – Equifax, Experian, and TransUnion – once every twelve months. The reports must contain all the information in an individual's file at the time of the request. *See* www.ftc.gov. These free credit reports can be accessed at the web site www.annualcreditreport.com.

In short, the FCRA as amended by the 2003 FACT Act, provides consumers with certain rights regarding the information in their credit reports. A credit report contains information about the individual's residence, credit account payment history, lawsuits, criminal, and bankruptcy history, among other things. Consumer reporting companies sell the information in credit reports to businesses that in turn use it to evaluate applications for a variety of things, such as credit, insurance, employment, or housing[407].

According to the FTC web site, the following points are notable with respect to credit reports:

- Since September 2005, on request, every individual is entitled to a free credit report on an annual basis from each of the main consumer reporting companies (Equifax, Experian, and TransUnion).[408]
- According to the FTC web site, federal law also entitles individuals to a free report if they are the subject of adverse action (*i.e.*, denial of a credit or employment application). In that case, the individual must request the report within 60 days of receiving notice of the adverse action. One free annual report is also available to individuals who are unemployed and plan to seek employment within 60 days or receives welfare, or if a report is inaccurate as a result of fraud, or identity theft.[409] A consumer can also receive a free credit report if he or she places a "fraud alert" on their credit file. Fraud alerts are discussed in the section on Identity Theft herein at Section V.F.

---

regulate, *e.g.*, the OCC is responsible for enforcing compliance with FCRA by the national banks it regulates. *See* 15 USCA § 1681s. State Attorneys General also have enforcement jurisdiction under the FCRA. 15 U.S.C. § 1681s(c).

407 *See* www.ftc.gov.

408 *See* www.ftc.gov.

409 15 U.S.C. § 1681 M.

- Consumers also have the right to learn which companies requested their report within the past year (up to two years for employment related requests).

- On denial of a credit application, a consumer can obtain the identity of the consumer reporting company that was contacted, if the denial was based on information given by the consumer reporting company.

- A consumer can file a dispute if he or she questions the accuracy or completeness of information in the credit report. The dispute can be filed with both the consumer reporting company and the information provider (the person, company, or organization that provided information about the consumer to the consumer reporting company), both of whom must investigate the claim and are required to correct any inaccurate or incomplete information in the report.[410]

- If the dispute is not resolved to the consumer's satisfaction he or she can append an explanation to the credit report, and for a fee, can have the explanation distributed to any prior recipients of the report.[411]

To obtain a consumer credit report, the entity requesting the credit report must have a "permissible purpose" as specified in FCRA. A person or entity requesting a consumer report (a "user") is required to certify its permissible purpose to the consumer reporting agency as a condition of receiving the report.[412] Knowingly obtaining a credit report under false pretenses is a criminal violation subject to fine or imprisonment.[413] Potential insurers, creditors and employers with whom the consumer has applied for a job or a financial product or service are typical "users" who are authorized to request and receive a credit report on individual. Consumer reporting agencies may also issue the report to users who certify that they have a legitimate business need for the information, either in connection with a business transaction that is initiated by the consumer; or to review an account to determine whether the consumer continues to meet the terms of the account. This requirement is apparent to anyone performing a

---

410 For details, *see* How to Dispute Credit Report Errors at www.ftc.gov/credit.

411 Excerpt from FTC Web site under "Facts for Consumers" available at the following link: http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre01.shtm. For consumers who wish to have additional information on how to order a free credit report see the following link to the FTC web site. *See also* http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre34.shtm.

412 15 USC § 1681b.

413 15 USC § 1681q.

search in the "Public Records" section of Westlaw or Lexis, where they are required to state the purpose for which the information requested (*i.e.*, non-commercial, or commercial in connection with a legal proceeding). Non-permissible uses will exclude certain information in a search, such as voter registration or drivers' license information. However, although access to the underlying information from Westlaw or Lexis is possible, this does not mean that such access is permissible or that a credit report can be obtained from these sources, which it cannot.

Even if a consumer has not requested insurance or credit, insurers and creditors can obtain a credit report if they agree to make a "firm" offer of credit or insurance.[414] This "firm offer" exception is the reason behind the frequent "preapproved" offers consumers receive. Consumer reporting agencies must provide a way for consumers to request that their names and information not be submitted in connection with such "pre-approved" solicitations.[415] A consumer may do so by calling 1-888-5-OPT-OUT. The removal election remains in effect for five years.

The FCRA also addresses identify theft, as addressed more fully below. (*See* Section V.F., infra).[416]

2. Affiliate Marketing Restrictions

a. Limiting Solicitations by Affiliates

The FCRA was later amended in 2003 by the FACTA.[417] One of the amendments gave consumers the right to restrict anyone from *using* certain information obtained from an affiliate to make solicitations to that consumer. In sum, if a business receives certain consumer eligibility information from an affiliate, that business may not use that information to make solicitations to

414 15 USC § 1681b.
415 15 USC § 1681b(e).
416 15 U.S.C. § 1681c-a.
417 *See* Pub.L. 108-159, 117 Stat.1952, 12/4/03.

the consumer unless the consumer is first given the right to "opt-out" and declines to do so. This prohibition, however, does not apply to affiliates who already have a pre-existing business relationship with the consumer, in situations where the consumer has requested the service or product or in cases where the affiliate is using the information to perform a service function for another affiliate. This opt-out provision may be no less than five (5) years, whereas the opt-out discussed above[418] regarding the *sharing* of information among affiliates under FCRA and the opt-out for the sharing of information among non-affiliates under GLB lasts until revoked by the consumer.[419]

FACTA governs the *use* of certain information – including experience and transaction information – by affiliates. It is therefore distinguished from the law concerning the *sharing* of information among affiliates[420] regarding the contents of a privacy policy under GLB.[421] Although distinct, the two statutes are related in that both require that the business in possession of the non-public customer information provide that customer with the right to "opt-out" before either: (1) sharing non-transactional or experience information with an affiliate (*e.g.*, credit report information, application information, etc. under FCRA;[422] or (2) allowing an affiliate to *use* any non-public personal information – including transactional and experience information to

---

418 *See* Section V.A.2. *supra*.

419 At the end of the mandated opt-out period, a consumer must be given the right to renew. As stated in the press release of the implementing regulations by the Fed: "Unlike the FCRA affiliate sharing opt-out and the Gramm-Leach-Bliley Act (GLBA) non-affiliate sharing opt-out, which apply indefinitely, Section 624 provides that a consumer's affiliate marketing opt-out election must be effective for a period of at least five years. Upon expiration of the opt-out period, the consumer must be given a renewal notice and an opportunity to renew the opt-out before information received from an affiliate may be used to make solicitations to the consumer." 72 F.R. 62911 11.07.07. Whether this should be a subject of further study and recommendation by NYSBA requires a more intense review to determine what legislative efforts may already be in progress.

420 Section V.A.2., *supra*.

421 S*ee also* FCRA 15 USC § 1681(d)(2)(A)(iii), which is referenced in the privacy regulations, *e.g.*, 12 C.F.R. 216.6 (a)(7).

422 15 USC § 1681a(d)(2)(A)(iii).

market the products or services of that affiliate.[423]

The FACTA required the federal bank agencies, National Credit Union Administration ("NCUA"), the FTC and the SEC to issue implementing regulations with a mandatory compliance date of October 1, 2008.[424]

b. Record Disposal

(i) Protecting Consumers from Unintended Dissemination of Information

The FACTA also amended FCRA to direct the FTC, the Fed and the other federal banking agencies, the NCUA and the SEC to coordinate and cooperatively adopt comparable and consistent rules regarding the disposal of sensitive consumer report information.[425] The intention was to reduce the risk of consumer fraud, including identity theft, created by improper disposal of any record that is, or is derived from, a consumer report. This imposes on those in possession of consumer information an affirmative duty to dispose of records or other forms of data which contain consumer information in a way that does not jeopardize the security of that data and prevents access to that information by unauthorized persons.

By way of example of the rules adopted by various federal agencies, the following is an example of the FTC rule that would be binding on all non-bank creditors:

(a) Standard. Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

(b) Examples. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples. These examples are illustrative only and are not exclusive or exhaustive methods for complying with the rule in this part.

---

423 15 USC § 1681s-3.

424 12 C.F.R. Part 41-OCC; 12 C.F.R. Part 222-Fed; 12 C.F.R. 334-FDIC; 12 C.F.R. Part 571- OTS; 12 C.F.R. Part 717-NCUA; 16 C.F.R. Parts 680,698 - FTC.

425 15 USC § 1681(w).

(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.

(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.

(3) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.

(4) For persons or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to this part, implementing and monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with examples (b)(1) and (2) of this section.

(5) For persons subject to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6081 *et seq.*, and the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule"), incorporating the proper disposal of consumer information as required by this rule into the information security program required by the Safeguards Rule.[426]

The bank agencies amended the Safeguards Rule to include a specific reference to the disposal of records containing consumer information. To that end, "consumer information" is defined as follows:

> Consumer information means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer

[426] 16 C.F.R. § 682.3.

> report and that is maintained or otherwise possessed by or on behalf of the bank for a business purpose. Consumer information also means a compilation of such records. The term does not include any record that does not identify an individual.[427]

Section II of the Safeguards Rule was also amended to expressly require the banks to "[E]nsure the proper disposal of customer information and consumer information."[428]

3. Enforcement of FCRA (including FACTA amendments to FCRA): Administrative and Private Right of Action

Administrative enforcement of FCRA is primarily delegated to the FTC and to other federal regulators, *e.g.,* the OCC will enforce violations of FCRA committed by a national bank. State officials including Attorney Generals may also bring actions against entities for violating FCRA and may seek damages on behalf of the injured consumer.[429] FCRA also permits private actions for certain violations and sets forth a formula for civil liability for willful noncompliance of the statute with respect to a consumer. Any person who willfully fails to comply with the statute with respect to a duty owed to a consumer may be liable to that consumer for the sum of actual damages sustained by the consumer or statutory damages in an amount not less than $100 and not more than $1,000. In the case of a natural person obtaining a credit report under false pretenses or without the proper authority, a consumer may receive the actual damages sustained by the consumer as a result of the failure or $1,000, whichever is greater. In either case, a consumer may also receive punitive damages as allowed by a court together with reasonable attorney's fees and costs for successful actions.[430] Civil penalties equal to actual damages plus attorney's fees and costs may also be awarded for cases of negligent violations of FCRA.[431] The FTC may also impose penalties under its own enforcement powers. Pursuant to the Federal Civil

---

427 Interagency Guidelines. *See, e.g.*, Fed regulations at 12 C.F.R. 208, Appendix D-2, I C 2 (b).
428 *See, e.g.*, Fed regulations at 12 C.F.R. 208, Appendix D-2, II 4.
429 15 USC § 1681s.
430 15 USCA § 1681n(a).
431 15 USCA § 1681o.

Penalties Inflation Adjustment Act of 1990, the FTC has increased certain maximum penalty amounts within its jurisdiction. The adjustments include an increase from $11,000 to $16,000 for civil penalties for unfair or deceptive acts or practices under the FTC Act, as well as an increase from $2,500 to $3,500 for credit reporting violations under the FCRA. These figures are maximum amounts and the FTC has the discretion to assess penalties in lesser amounts. The increases became effective February 9, 2009.

C. The Children's Online Privacy Protection Act

As discussed further in Section I. B., enforcement of COPPA is primarily delegated to the FTC, or, in the case of particular entities, the functional federal regulator (*e.g.*, the way that OCC has the right of enforcement over national banks).[432] State Attorneys General may bring an action under COPPA where they believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates a regulation of the FTC.[433]

D. The Drivers Privacy Protection Act

The Drivers Privacy Protection Act[434] ("DPPA") prohibits any state agency like the Department of Motor Vehicles from selling or otherwise releasing drivers' license numbers and related information contained in driver records except for limited purposes such as fraud prevention and insurance claim investigations.[435] The statute also prohibits any person from knowingly obtaining information from a motor vehicle record on false pretenses and prohibits anyone from obtaining or disclosing personal information, from a motor vehicle record, for any use not expressly authorized by law. A person who knowingly obtains, discloses or uses

---

432 *See* discussion I.B, *supra*. 15 USC § 6505.
433 15 USC § 6504.
434 18 USC §§ 2721, *et seq*.
435 18 USC §§ 2721, *et seq*.

personal information from a motor vehicle record for a purpose not permitted under this statute is liable to the individual to whom the information pertains. That "victim" may bring a civil action in a United States district court and the court may award actual damages, but not less than liquidated damages in the amount of $2,500; punitive damages upon proof of willful or reckless disregard of the law; reasonable attorneys' fees and other litigation costs reasonably incurred and such other preliminary and equitable relief as the court determines to be appropriate.[436] Any State agency that violates this federal law may be sued by the Attorney General and is subject to a fine of up to $5,000 per day.

E. Enforcement Actions by the Federal Trade Commission Under Section 5 of the FTC Act

As discussed in greater detail in Section V. B. I. herein, the FTC has brought enforcement proceedings against companies that do not adequately protect their customers' personal information on grounds that such failure constitutes an unfair trade practice under Section 5(a) of the FTC.[437] The FTC has also taken the position that inadequate data security may also constitute a deceptive trade practice if it is inconsistent with the company's privacy notice.

In November, 2008, the FTC announced a settlement with a mortgage company, Premier Capital Lending, Inc. ("Premier"), after charging that Premier had engaged in deceptive practices by failing to safeguard customer data as required by the FTC regulations implementing GLB privacy rules for non-bank creditors. The following is an excerpt from the FTC press release:

> A Texas-based mortgage lender has settled Federal Trade Commission charges that it violated federal law by failing to provide reasonable security to protect sensitive customer data. The lender made the data vulnerable, the complaint alleges, by allowing a third-party home seller to access the data without taking reasonable steps to protect it. A hacker compromised the data by breaking into the home seller's computer, obtaining the lender's credentials, and using them to access hundreds of consumer reports.

---

436 18 USCA § 2724.

437 Act 15 USC § 45.

According to the FTC's complaint, the lender violated the FTC's Safeguards and Privacy Rules, as well as Section 5 of the FTC Act. The proposed settlement bars deceptive claims about privacy and security, and requires the company to establish a comprehensive information security program and hire an independent third-party security professional to review the program every other year for 20 years.

The FTC complaint alleges that Premier violated the Safeguards Rule because it: allowed a home seller to use its account for accessing credit reports in order to refer purchasers for financing without taking reasonable steps to verify the seller's procedures to handle, store, or dispose of sensitive personal information; failed to assess the risks of allowing a third party to access credit reports through its account; failed to conduct reasonable reviews of credit report requests made on its account by using readily available information (such as management reports and invoices) to detect signs of unauthorized activity; and failed to assess the full scope of credit report information stored and accessible through its account and thus compromised by the hacker.

According to the FTC, a hacker exploited Premier's failures by breaching the seller's computer, obtaining Premier's user name and password, and using these credentials to obtain at least 400 credit reports through Premier's account.

The FTC complaint also alleged that Premier violated Section 5 of the FTC Act and the Privacy Rule by failing to live up to its own privacy policy, which claimed: "We take our responsibility to protect the privacy and confidentiality of customer information very seriously. We maintain physical, electronic, and procedural safeguards that comply with federal standards to store and secure information about you from unauthorized access, alteration and destruction. Our control policies, for example, authorize access to customer information only by individuals who need access to do their work."[438]

The FTC has also brought charges against businesses based solely on what it considered a "deceptive practice" regarding their handling of consumer non-public personal information. For example, in March 2008, the FTC announced that in two unrelated FTC actions involving discount retailer TJX and data brokers Reed Elsevier and Seisint.[439] Each party agreed to settle charges that they had engaged in practices that, taken together, failed to provide reasonable and

---

438 FTC Press release 11.08.08 at: http://www.ftc.gov/opa/2008/11/pcl.shtm. The FTC complaint in *In the Matter of Premier Capital Lending, Inc. and Debra Stiles*, FTC File NO. 0723004, Docket No. C-4241, is available at http://www.ftc.gov/os/caselist/0723004/081206pclcmpt.pdf.

439 In the matter of the TJX Companies, Inc., FTC File No. 072-3055 and in the matter of Reed Elserier, Inc. and Seisint, Inc., FTC File No. 052-3094, available at http://www.ftc.gov/os/caselist/0723055/index.shtm and http://www.ftc.gov/05/caselist/0523094/index.shtm.

appropriate security for sensitive consumer information. The settlements require that the companies implement comprehensive information security programs and obtain audits by independent third-party security professionals every other year for 20 years.[440]

While consumer groups would argue that greater safeguards against "hackers" should be built into the GLB or the FTC's standards, businesses would argue that they are already doing as much as is cost-effectively possible. Whether the "reasonable measures" standard to protect against unauthorized access to or use of consumer information is sufficient remains an open question for the legislatures to address. It would appear that some states – including New York – did not consider the federal law to be sufficient because those states adopted their own data security breach laws compelling businesses (and, in some cases, government agencies) to advise the individuals (and other regulators/law enforcement officials) when personal information is compromised.[441]

F. Laws, Regulations, and Case Law Involving Data Security and Identity Theft

"Identity theft" is defined by the FTC as "a fraud committed or attempted using the identifying information of another person without authority."[442] Identity theft is a federal crime

---

440 *See* FTC Press Release dated March 27, 2008, available at: http://www.ftc.gov/opa/2008/03/datasec.shtm. A listing of all FTC cases can be obtained at: http://www.ftc.gov/os/index.shtml. Future privacy initiatives would be well served to revisit the issue of whether there should be greater safeguards built into the GLB or the FTC's standards against hackers and whether the statute and standards have been effective in detecting and prosecuting persons who intentionally obtain unauthorized access to information. This is especially notable given that the relatively low number of complaints brought by the FTC seems disproportionate to the number of data breach incidents reported in the media, and does not seem effective to prevent widespread tampering.

441 The FTC is generally considered to be aggressively pursuing privacy issues and safeguarding private data, and Task Force members and other sources have, which oversees a board range of commercial issues beyond privacy commented that it does so despite a limitation of resources. For example, the FTC recently pursued a case against Choice Point that resulted in a combined $15 million in civil penalties and consumer redress. *See* http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

442 16 C.F.R. § 603.2(a).

punishable by two to five years in prison[443] and is a crime under most state laws as well.[444]

The "Red Flags Rule" is another FACTA required regulation issued by the FTC and federal banking regulators. Both the FTC and federal banking regulators issued the so-called "Red Flags Rule" that requires financial institutions and creditors who establish or maintain "covered accounts" (open and closed-end consumer credit accounts involving multiple payments or transactions and certain deposit and business credit accounts having the potential for identity theft) to develop and implement a written Identity Theft Prevention Program ("ITPP") to detect, prevent, and mitigate identity theft when opening and monitoring covered accounts. Entities like retail stores that offer "instant credit" charge card programs, medical providers who establish payoff plans, and auto dealers who originate contracts for indirect auto finance are all subject to the "Red Flags" Rule.

A risk-based ITPP must be "appropriate to the size and complexity of the [institution] and the nature and scope of its activities."[445] The initial ITPP must be approved by the Board of Directors (or a committee of the Board) and an annual report must be made to the Board concerning the ITPP's effectiveness. Among other things, the ITPP must contain procedures to: (i) identify patterns, practices or specific activity that indicate the possible existence of identity theft (these being the institution's "red flags"); (ii) detect the presence of any red flags in customer transactions and account activity; (iii) respond appropriately to detected red flags to detect, prevent and mitigate identity theft; and (iv) ensure the ITPP is periodically updated to reflect experiences and changes in patterns of identity theft.[446] Related regulations require

---

443 18 U.S.C. § 1028A.

444 *E.g.*, N.Y. Penal Law §§ 190.78 -.80; Conn. Gen. Stats. § 53a-129a.

445 16 C.F.R. § 681.2(d).

446 The Red Flags Rule is published in 16 C.F.R. Part 681 (FTC); 12 C.F.R. Part 41 (OCC); 12 C.F.R. Part 222 (Federal Reserve Board); 12 C.F.R. Parts 334 and 364 (FDIC); 12 C.F.R. Part 571 (OTS); and 12 C.F.R. Part 717 (NCUA).

creditors to resolve notices of address discrepancies they receive when they pull a customer's credit report and impose obligations on card issuers who receive requests to issue additional or replacement cards within 30 days after receiving a change of address for a card account.[447]

1. Interagency Guidance for a "Response" Program, including Customer Notification of Unauthorized Access to Customer Information

As part of the federal bank agency Safeguards Rule for the safeguarding of customer information discussed above, the bank agencies have also issued a joint "Guidance" which describes the response program, including customer notification procedures, that a financial institution should use to address unauthorized access to or use of customer information that could result in "substantial harm or inconvenience to the customer."[448] At minimum, the response program should contain procedures for the following:

(a) Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;

(b) Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;

(c) Consistent with the [Bank] Agencies' Suspicious Activity Report ("SAR") regulations (*see* 12 C.F.R. § 208.62 for banks regulated by the Fed requiring appropriate notifications to law enforcement authorities), in addition to filing a timely SAR in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

(d) Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and

(e) Notifying customers when warranted.[449]

---

447 *See, e.g.*, 16 C.F.R. 681.1 (Address Discrepancy Rule) and 681.3 (Duties of card issuers regarding changes of addresses).

448 12 C.F.R. Part 208, Supplement A to App. D-2.

449 12 C.F.R. Part 208, Appendix D-2, Supplement A II.

While the Guidance notes that notifying customers of a security incident involving the unauthorized access or use of the customer's information is important to the institution in managing its reputation risk and important to the customers by allowing them to take steps to protect themselves against the consequences of identity theft, notification is not always strictly required each time there is any type of security breach. The standard for notification is the unauthorized access to or use of customer information that could result in "substantial harm or inconvenience" to any customer through improper access to "sensitive customer information". The Guidance further provides as follows:

> Substantial harm or inconvenience is most likely to result from improper access to *sensitive customer information* because this type of information is most likely to be misused, as in the commission of identity theft. For purposes of this Guidance, *sensitive customer information* means a customer's name, address, or telephone number, in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. *Sensitive customer information* also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.[450]

If the financial institution can identify those customers whose information has improperly been accessed, the notice need only be sent to those individuals. However, if the financial institution cannot determine which specific customers have been affected, then it must send the notice to all customers in the group which the institution determines has or may have been affected. The customer notice should be given in a "clear and conspicuous" manner. It should describe the incident in general terms and the type of customer information to which there was

[450] 12 C.F.R. Part 208, Appendix D-2, Supplement A III (emphasis in the original). This leaves open the possibility that a customer will not be notified of a security breach if it is ultimately determined that the breach does not rise to the level of the "substantial harm or inconvenience" standard. Further study of this point may be warranted, particularly to consider what constitutes "substantial harm or inconvenience".

unauthorized access. It should also describe what steps the financial institution has taken to safeguard the information from further unauthorized access and provide a telephone number that customers can call for additional information and assistance. The notice should also remind customers that they need to monitor their credit report during the following 12 to 24 months and to promptly report incidents of suspected identity theft to the financial institution.

The Guidance also provides that the notice should include the following information as appropriate under the circumstances:

> (f) A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;
>
> (g) A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;
>
> (h) A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
>
> (i) An explanation of how the customer may obtain a credit report free of charge; and
>
> (e) Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.[451]

The Guidance allows the financial institution to deliver the notice in any manner designed to ensure that the customer will receive it including by telephone, mail, or for those customers who have agreed to receive communications electronically and for whom the institution has a current e-mail address, sending the notice electronically.

As noted above (*see* Section V.A.2, supra), Title V of GLB and the implementing

[451] 12 C.F.R. Part 208, Appendix D-2, Supplement A III (B).

regulations are subject to enforcement by the functional regulator of the particular financial institution, although the GLB does not provide for a private right of action.

2. Overview of State Data Security Breach Notice Laws

Companies that are not regulated financial institutions may be subject to a myriad of state laws requiring notice to residents of their states in the event of a security breach of customer information. These laws are not consistent in terms of when and how notice is required, whether there is any threshold of harm standard for giving notice and the penalties, rights or causes of actions or other relief for failing to comply. A "one size fits all" notice form is therefore unlikely to provide a workable solution.[452] In New York, General Business Law § 899-aa authorizes the Attorney General to bring an action for damages, including consequential damages for failing to provide the proper requisite notice. If the violation is knowing or reckless, the Court may also impose a civil penalty of the greater of $5,000 or $10 per failed notification (up to $150,000). New York City also has a data security breach notification law.[453]

States have also enacted new laws and regulations requiring additional security measures and liability risks for entities that do not adequately protect the personal information of state residents. For example, Minnesota's "Plastic Card Security Act"[454] prohibits a merchant from retaining for more than 48 hours from transaction approval any payment card CVC or CVV codes (the 3-digit code imprinted on the signature panel of a card), the PIN verification code of a debit card or any information derived from a card's magnetic stripe. If the merchant retains this information for longer and its database is compromised, card-issuing banks have a cause of action against the merchant for their costs of reissuing compromised cards (about $20 per card),

---

452 *For example*, New York and California do not have any threshold of harm before a notice is required.

453 N.Y.C. Administrative Code § 20-117.

454 Minn. Stat. ch.325E, § 64.

crediting certain unauthorized charges back to the cardholder, and giving notices of the breach to their cardholders.

A Massachusetts law and enabling regulations effective January 1, 2010 will require that any person or entity that owns, licenses, stores, or maintains personal information about Massachusetts residents to develop a comprehensive written information security program containing at least 11 separate required provisions.[455] This law and regulations are very specific in terms of what the security program and computer system must include, and it extends beyond the requirements of GLB regulations. Among other requirements, all Massachusetts residents' information must be secured using sophisticated technology measures, such as encrypting personal information whenever it is transmitted electronically or stored in any laptop computer, flash drive or portable device. The regulations also mandate audits of employee access to personal information, and prescribe specific minimum requirements for data security systems. The Massachusetts Attorney General is authorized to sue for a violation of this law as an unfair trade practice and obtain injunctive relief, treble damages, a civil penalty of $5,000 per violation, plus costs of investigation and attorney's fees.[456]

Nevada law also requires encryption of all personal information of a customer in electronic transmissions.[457]

Many states, including New York, have Social Security number protection laws that require companies to protect Social Security numbers that they possess in their business. For example, New York's General Business Law Section 399-dd prohibits printing, communicating, encoding on a card or requiring for web site access any person's Social Security number, defined as the unencrypted full number or any number derived from it such as the last 4 digits. Under

---

455 Mass. Gen. Laws ch. 93H, § 2(a); 201 Mass. Reg. Code tit.17.00.

456 Mass Gen. Laws ch. 93H, § 6, ch. 93A, § 4.

457 Nev. Rev. Stats. § 597.970.

New York's law, the Attorney General may bring a special proceeding for an injunction, restitution and civil penalties of up to $1,000 per violation not exceeding $100,000 for all violations resulting from a single act, and seek $5,000 per subsequent violation not exceeding $250,000 for those violations resulting from a single act.

Other states have similar laws protecting Social Security numbers. State laws generally require Social Security numbers to be protected, encrypted in any electronic transmission and, in some states, encrypted in storage as well. Like New York, most of these laws prohibit using Social Security numbers as identifiers or publishing Social Security numbers on identification cards, or in mailings. Connecticut's law requires companies to post on their Internet web site or otherwise publish a public privacy protection policy that describes how the company protects the confidentiality of Social Security numbers, prohibits their unlawful disclosure, and limits access to them.[458] A company that intentionally violates the Connecticut law is subject to a civil penalty of $500 per violation, not to exceed $500,000 per single event.[459] Michigan, New Mexico, and Texas laws are to similar effect but do not require publication of the privacy protection policy.[460] State Social Security number and data protection laws contain different definitions of information subject to protection and are not uniform.

3. Litigation Involving Data Security Breaches

Persons whose identities have been compromised in data security breaches have generally not been successful in litigation unless they can show that they personally suffered an identity theft that can be linked to the data breach itself. Lawsuits involving data security breaches have alleged claims such as negligence, breach of an express or implied contract (typically, the company's privacy policy), breach of fiduciary duty, and statutory consumer

458 2008 Conn. Pub. Acts 08-167.

459 Id.

460 Mich. Comp. Laws § 445.84; N.M. Stat. Ann § 57-12B-3; Tex. Bus. & Com. Code § 35.581.

protection laws such as unfair and deceptive trade practices. Courts have generally found no compensable damages merely for the fear of identity theft or the cost of credit monitoring services.[461] However, where the plaintiff has been the subject of identity theft and can directly link the defendant's conduct to the identity thief, courts have allowed causes of action to proceed.[462]

Recent litigation trends may suggest a possible loosening of some of these standards for recovery. TJX Corporation, which suffered the compromise of an estimated 95 million payment cards over a four-year period due to inadequate data security practices, paid $41 million to Visa and $24 million to MasterCard to settle claims by their card issuers to recover costs of card reissuance and unauthorized charges. TJX also agreed to settle a consumer class action brought by persons whose cards had been compromised for an amount in excess of $100 million covering various forms of payments, credits, and card monitoring services. Claimants will not be required to prove that TJX was the cause of their card compromise nor prove actual damages as most courts have previously required. Following the security breach, TJX was reported to have publicly urged banks and other retailers to implement a new but costly micro-chip technology to prevent credit and debit card theft. 2008 WLNR 16453546, Boston Globe, 8/31/08.[463]

---

461 *E.g., Pisciotta v. Old National Bancorp*, 499 F.3d 629, 639 (7th Cir. 2007) (citing other cases); *Shafran v. Harley-Davidson, Inc.*, 2008 U.S. Dist. LEXIS 22494 (S.D.N.Y. March 24, 2008) (Motion granted to dismiss a class action complaint based upon a lost laptop, the Court ruling that credit monitoring costs sought by plaintiff to protect against a yet-to-occur injury could not constitute an actual and legally cognizable injury).

462 *E.g., Bell v. Michigan Council 25 of the American Federation of State, County and Municipal Employees*, 2005 Mich. App. LEXIS 353 (Ct. App. Feb. 15, 2005), appeal dismissed, 474 Mich. 989 (2005) (a union employee brought home personal employee information that was accessed by her daughter, who then used the information to commit identity theft for which she was criminally convicted; the union was held liable to the victims); *Daly v. Metropolitan Life Insurance Co.*, 4 Misc.3d 887, 782 N.Y.S.2d 530 (Sup. Ct. N.Y. Co. 2004) (Janitor stole plaintiff's life insurance application from a desk in defendant's warehouse and used plaintiff's identity to open credit card accounts in plaintiff's name at the janitor's home address).

463 By way of a post-script to the TJX debacle, the federal authorities issued charges against the identity theft ring allegedly responsible for the theft and sale of several million credit and debit card numbers from TJX and other retailers. *See* 8/6/08 Boston Herald 22 (2008 WLNR

Additionally, the Third Circuit Court of Appeals reversed the dismissal of a breach of contract lawsuit by Sovereign Bank, issuer of cards compromised in the BJ's Wholesale Clubs security breach in 2004.[464] Sovereign sued BJ's and its merchant acquirer, Fifth Third Bank, for breach of contract alleging that Sovereign was a third party beneficiary of Visa's operating rules that mandated card security practices breached by BJ's and Fifth Third. The Third Circuit held that there were material issues of fact on the contract claim against Fifth Third Bank by reason of its failure to ensure that BJ's complied with Visa rules on retaining cardholder information.

A New Jersey case, *Brunson v. Affinity Federal Credit Union*,[465] ruled that a financial institution that pursues criminal charges against an innocent third party whose identity is stolen and used to defraud the bank can be sued for negligence and malicious prosecution. In this case, an identity thief used the plaintiff's name, birth date and Social Security number to open an account and defraud the credit union. The credit union swore out criminal charges and the plaintiff was incarcerated for thirteen days before the complaint was dismissed. The court ruled that the plaintiff, even though not an account holder, was owed a duty by the credit union when it opened an account in his name. "Financial institutions – particularly banks – have a duty to exercise reasonable care in opening accounts. . . That duty included the duty to conduct a reasonable investigation before initiating criminal proceedings against the person whose stolen identity was used to open the account."[466] The Red Flags Rule, discussed in Section III. F. herein, effectively codifies this duty under federal law.

These cases may portend a greater risk of liability to entities when personal customer information is compromised.

14703817).

464 Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162 (3d Cir. 2008).

465 *Brunson v. Affinity Federal Credit Union*, 402 N.J. Super. 430, 954 A.2d 550 (App. Div. 2008).

466 *Id.* at 564.

4. Security Freeze Laws

Forty-eight states, including New York, have laws that allow consumers to "freeze" their credit report files, making them unavailable to prospective new creditors such as credit card companies, auto dealers and retailers although the three major credit bureaus also now give this right to consumers in all states. New York's credit freeze law is discussed more fully immediately below.

G. New York State Statutes Affecting Financial Privacy: Description of Statutes that Impose a Duty Regarding the Collection and Disposal of Customer Information

1. Confidentiality of Social Security Account Numbers

As further discussed herein, Social Security numbers were never intended to be used as identifiers. Yet, in practice, they have become just that, and have become a breeding ground for identity theft. As a result, New York law prohibits from communicating or publicly displaying an individual's Social Security account number or some portion of it. For example, businesses are prohibited from printing the Social Security number on any card or tag required for a person to access products, services or benefits. Similarly, no business can require an individual to transmit a Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted. Social Security numbers may not appear on documents mailed to individuals unless state or federal law requires the Social Security number to appear on the document. However, the statute expressly allows the Social Security number to appear on an application and other forms sent by mail provided that the number is not visible to the general public. Therefore, the Social Security number cannot appear on a post card or the outside of the envelope.[467]

GBL § 399-dd has been amended, effective January 1, 2009, to add two additional

[467] New York General Business Law ("GBL") § 399-dd (added L. 2006, Ch. 676).

prohibitions regarding the use of a Social Security number:

1. A business may not encode or embed a Social Security number in a card or document such as through the use of a bar code or magnetic chip; and

2. No public document filed with any state agency or political subdivision or in any court in New York may contain a Social Security number unless that person is a dependent child or has consented to such filing – unless the display of the Social Security number is required by state or federal law or regulation or by court rule.[468]

The statute authorizes the Attorney General to commence enforcement proceedings and authorizes a court that determines a violation has occurred to impose a civil penalty of not more than $1,000 for a single violation and not more than $100,000 for multiple violations resulting from a single act or incident. Any subsequent violations may be punishable by a civil penalty of not more than $5,000 for a single violation and not more than $250,000 for multiple violations resulting from a single act or incident. There is also a safe harbor for businesses that can show the violation was not intentional and resulted from a bona fide error made despite the entity's maintenance of procedures reasonably adopted to avoid such error.[469]

2. Government Prohibitions Regarding Social Security Numbers

Effective January 1, 2010, New York State and its political subdivisions will also be prohibited from publicly displaying an individual's Social Security account number on any document or access device where the account number will be visible to the general public. Mailings may only include the last four digits of a Social Security number unless a federal or state law requires otherwise. Electronic mail that is copied to third parties may only contain the last four digits of a Social Security number. In addition, the government may not require a person to transmit the Social Security number over the Internet unless the connection is secure or

[468] L. 2008 Ch.279, adding NY GBL § 399-dd (2) (f) and a new (6) and renumbering old (6) as (7).
[469] NY GBL § 399-dd (7).

the Social Security number is encrypted.[470] This statute does not have any express enforcement section.

3. Employers and Social Security Numbers

Effective January 3, 2009, an employer is prohibited from: publicly displaying or posting an employee's Social Security number; visibly displaying the account number on any badge or card including a time card; placing a Social Security number in files with unrestricted access; or communicating an employee's personal identifying information to the general public. The statute defines such information to include: an employee's Social Security number, home address, personal e-mail address, Internet name or password, drivers' license number, or parent's surname prior to marriage.[471]

The Commissioner of the Department of Labor may impose a civil penalty of up to $500 on any employer for a knowing violation of this law. It will be presumptive evidence that a violation was "knowing" if the employer has not put into place any policies or procedures to safeguard the employee's personal identifying information.[472]

4. Sale of Telephone Records

No business or person may obtain, sell, or use telephone record information (land lines and wireless) without the authorization of the customer. This prohibition is not applicable to information sought or obtained by a subpoena, law enforcement agency or telephone company in compliance with other law or in the performance of official duties in accordance with other applicable laws. The policy statement which led to the adoption of this statute provides that telephone customers have a right and expectation of privacy not only with respect to the content

470 NY Public Officers § 96-a (L. 2008, Ch.279, § 3).
471 NY Labor Law § 203-d (L. 2008, Ch, 279, § 6, eff. January 3, 2009); *see also* Section IV. herein.
472 NY Labor Law § 203-d (3).

of their telephone calls, but with respect to information concerning them such as the telephone numbers called, the length of the calls, the numbers from which calls are received, etc.[473]

The statute authorizes the Attorney General to commence enforcement proceedings and authorizes a court that determines a violation has occurred to award reasonable attorney's fees and damages for actual costs or losses. The court may also impose a civil penalty of $1,000 per violation.[474]

5. Proper Disposal of Records Having Personal Identifying Information

A business entity (excluding the state or its political subdivisions) is prohibited from disposing of a record containing personal identifying information unless that entity, or other person under contract with the entity, does any of the following:

- Shreds the record prior to disposal;
- Destroys the personal identifying information contained in the record;
- Modifies the record to make the personal identifying information unreadable; or
- Takes actions consistent with commonly accepted industry practices that it reasonably believes will "ensure" that no unauthorized person will have access to the personal identifying information in the record.[475]

"Personal identifying information" is defined to mean any personal information which can be used to identify a person (because of name, number, personal mark or other identifier) in combination with any one or more of the following data elements when either the personal information or the data element is not encrypted or encrypted with the an encryption key that is included in the same record as the encrypted personal information or data element: (1) Social Security number, (2) driver's license number or non-driver identification card number; or

473 NY GBL § 399-dd, L. 2006, Ch. 487. (Note-there are two § 399-dd provisions).
474 NY GBL § 399-dd (3).
475 New York Disposal of Personal Records Law (New York General Business Law § 399-h.

(3) mother's maiden name; financial services, checking, or savings account number/code, automated teller machine number/code; debit car number or code; electronic serial number or personal identification number.[476]

The Attorney General is authorized to seek a court order to enjoin and restrain a business from violating the Act. A court may impose a fine of as much as $5,000 if it determines that a business has not disposed of the records as required. Acts arising out of the same incident constitute a single violation. It is an affirmative defense if the business can show that it used due diligence in its attempt to properly dispose of such records.[477]

6. A Consumer's Right to Impose a Security Freeze on Their Credit Report

In 2006, New York enacted a law allowing consumers to direct a consumer credit reporting agency (a "CRA") to place a "security freeze" on their consumer credit reports by sending a written request to a CRA by certified or overnight mail. Consumers can "thaw" their frozen credit reports either for specific creditors or for designated periods of time simply by calling the credit bureau and using a PIN given to them by the credit bureau at the time the consumer initially froze their credit file. This thawing process can take less than five minutes but requires use of the PIN. New York's law allows consumers to freeze their credit files at each of the three national credit bureaus – for free; effective January 1, 2009 consumers can do so by mail, telephone or the Internet.[478] The revised provision states as follows:

---

476 NY GBL § 399-h. GBL § 399-h was amended in 2008 (L. 2008, Ch. 516) to clarify that while it applies to not-for-profit corporations and entities, it does not apply to individual persons who are not engaged in a business for profit. Thus, a person may dispose of their own family records and be exempt from the reach of the statute.

477 NY GBL § 399-h (3).

478 N.Y. Gen. Business Law §§ 380-a, 380-t; *See* http://www.consumer.state.ny.us/security_freeze.htm containing additional details and sample letters to send to each credit bureau to freeze a credit file; *see also* www.equifax.com, www.experian.com, and www.TransUnion.com. Freezing a credit file will not opt a customer out of "prescreening" whereby a creditor obtains from the credit bureau a list of names and addresses of consumers to send pre-approved firm offers of credit such as credit card offers. To be removed from prescreening, a consumer must call 1-888-5-OPTOUT (1-888-567-8688).

> A consumer may request that a security freeze be placed on his or her consumer credit report by sending a request in writing with confirmation of delivery requested or via telephone, secure electronic means, or other methods developed by the consumer credit reporting agency to a consumer credit reporting agency at an address, telephone number or secure web site designated by such agency to receive such requests. Consumer credit reporting agencies shall have a secure web site and a separately dedicated toll-free number to offer information, to process requests and deliver the services provided for under this section.[479]

Consumers may direct the CRA to temporarily "lift" the freeze and thereby allow their credit report to be accessed for a specified party or for specified period of time after which the freeze will remain in place. CRAs are required to honor this request within three business days once the consumer has provided them with proper identification, the unique personal identification number or password the CRA must provide to all who request a security freeze, proper information about the time period or party to whom the temporary "lift" applies and payment of any applicable fee. Effective September 1, 2009, a request to "lift "the freeze that is received by telephone or via e-mail must be honored within fifteen minutes.[480]

The security freeze provisions do not apply to certain categories of entities including: existing creditors, persons to whom a financial obligation (*i.e.*, debt or judgment) is owed, government entities, child support agencies, law enforcement, check service or fraud prevention companies, credit monitoring services and individuals accessing their own credit files.

Any time a CRA is required to send a summary of rights under federal law[481] to a consumer residing in New York, the CRA has to include a summary of these additional rights in the model form entitled: "NEW YORK CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE."

---

479 NY GBL § 380-t as amended by L. 2008, Ch.279 § 2.

480 NY GBL § 380-t (e), as amended by L. 2008 Ch. 279 § 2.

481 15 U.S.C. § 1681g.

With a few exceptions, CRAs are permitted to charge consumers who have not filed a police report or an affidavit with the FTC or a law enforcement agency alleging identity theft, a fee of up to $5 for the removal or lifting of a freeze, for the second or any subsequent placement of a freeze (there can be no fee for the first freeze), or the replacement of a PIN or password.[482] The statute was amended effective August 5, 2008 to allow victims of domestic violence to request a security freeze on their credit reports and CRAs are prohibited from charging a fee for this service.[483]

CRAs may remove the security freeze at the consumer's request (following proper identification of the person requesting the removal). CRAs may also remove the security freeze if the consumer credit report was frozen "due to a material misrepresentation of fact by the consumer." Before removing the freeze for this latter reason however, the CRA must first notify the consumer in writing.

The State Attorney General is authorized to commence an action against anyone who violates this statute seeking a court order to enjoin and restrain the continuance of such violations. A court may impose a civil penalty of not more than $5,000 per violation.[484]

7. Fair Credit Reporting Act

New York has its own "mini" Fair Credit Reporting Act NY.[485] Although much of it has been preempted by the enactment of the federal Fair Credit Reporting Act or FCRA (discussed at V. B, *supra*), New York offers an additional consumer protection by requiring entities to disclose that a consumer report may be ordered in connection with certain kinds of applications – before the report is ordered by the user (*e.g.*, creditor, insurer, etc.).

---

482 NY GBL § 380-t (2).

483 NY GBL § 380-t, L. 2008 Ch. 406.

484 NY General Business Law § 380-t, L. 2006, Ch. 63, initially effective 11/01/06, amended L. 2008, Ch. 279; L. 2008, Ch. 406.

485 GBL § 380, *et seq*.

No person or entity may request or use a credit report in connection with an application for credit, employment, insurance, or rental or lease of residences unless that entity first discloses to the applicant that a consumer credit report may be ordered on the applicant in connection with the application. This notice must further disclose that at the consumer's inquiry, the entity will advise whether a report was ordered and if one was, will supply the name and address of the CRA. This disclosure typically appears on the application form or on a document within the application package. If the application is in writing the notice must also be provided in writing.

If the entity also discloses that subsequent reports may be requested or utilized in connection with an update, renewal, or extension of the credit, employment, insurance, or rental or lease of residences for which application was made, no additional notice to the consumer is required to be sent at the time such subsequent report is requested.[486]

H. Data Security Breach Laws

Data Security Breach laws impose on both government agencies and private business entities an obligation to act when personal information is lost or potentially compromised. The laws as applied to private businesses and government agencies is discussed below.

1. Private Businesses

Any person or entity that conducts business in New York and owns or licenses computerized data which includes "private information" is required to disclose any breach of the security of the system. A "breach" is considered to have occurred upon the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the business. The disclosure to the affected person – and other agencies – must be made "in the most expedient time possible and without unreasonable delay."

[486] NY GBL § 380-b (b).

"Private information" is statutorily defined as (i) information which can identify a natural person (*e.g.*, name, number, personal mark) plus (ii) any one or a combination of the data elements set forth below when either the identifying personal information or the data element is not encrypted, or if it was encrypted with an encryption key that has also been acquired:

> (1) Social Security number;
>
> (2) driver's license number or non-driver identification card number; or
>
> (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.[487]

Notice must be given in writing, by electronic notice if the recipient has consented to receiving notices in electronic form, or by telephone provided a log is kept of those who have been contacted. If a business can demonstrate to the Attorney General that the cost of providing the notice may exceed $250,000, that the affected class of persons exceeds 500,000 or that the business lacks sufficient contact information, a form of "substitute notice" may be arranged including notification to statewide media, posting on the business web site, etc.

The "notice" must include contact information for the person or business making the notification and:

> a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.[488]

The business must also notify the State Attorney General, the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content and distribution of the notices and approximate number of affected persons. If more than 5,000 New York residents are to be notified, the business must also notify consumer

---

[487] NY GBL § 899-a(1)(b).

[488] NY GBL § 899-aa (7).

reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons.[489]

Whenever the Attorney General believes that this law has been violated, he or she may bring an action to enjoin and restrain the continuation of the violation. A court may then award damages for actual costs or losses, including consequential losses. If the violation is found to be knowing or reckless, the court may also impose a civil penalty of the greater of $5,000 or $10 per failed notification up to $150,000.

The Office of the Attorney General recently settled with CS STARS LLC, a claims management company that failed for seven weeks to notify either the owner of the computerized data or 540,000 New York consumers whose personal information was at risk. A CS STARS computer containing the personal information of recipients of worker's compensation benefits went missing, but the company failed to notify the owner of the data, the potentially affected consumers or the state entities as required by law. As part of the settlement in which no wrongdoing was admitted, CS STARS agreed to comply with the law (issue the required notices) and to also pay $60,000 for costs related to the investigation.[490]

2. State Data Security Breaches.

There is a similar data security breach notification law which is binding on any New York State agency, department, division, authority or political subdivision which has personal information on a computerized data system which is lost or compromised. The notice requirements are similar to those imposed on private businesses, although there is no separate

---

489 NY GBL § 899-aa; the web site of the Cyber Security and Critical Infrastructure Coordination provides a sample form of notification to it and the other state agencies plus additional information. http://www.cscic.state.ny.us/security/securitybreach/.

490 *See* http://www.oag.state.ny.us/media_center/2007/apr/apr26a_07.html.

provision regarding enforcement.[491]

3. New York City's Data Security Breach Notification Law

New York City has its own data security breach notification law. It applies to persons or entities licensed by the New York City Department of Consumer Affairs ("DCA") or any business over which the DCA has regulatory authority which has "personal identifying information" that has been accessed or obtained by an unauthorized person/entity. Unlike the New York State law, this obligation to notify the consumer of a data security breach is not limited to the breach of security with respect to computerized data maintained by the business, but applies to all such data no matter the form in which the information is maintained, such as a breach of paper files containing personal identifying information. Should a breach occur, the business is required to notify the affected person, plus the DCA and the New York City Police Department. The Administrative Code does not specify any requisite content of the notice to the consumer.[492] If a person or business subject to licensure or regulation by the DCA is found guilty of failing to comply with this provision of the administrative code, that entity may be fined not more than $500 and be liable for a civil penalty of $100 per violation.[493]

I. Identity Theft

1. Protecting the Military

It is an "aggravated identity theft" and a Class D felony to knowingly and with intent to defraud, use the personal identifying information or assume the identity of a person who is a member of the armed services who is deployed outside of the country in obtaining goods, services, credit or otherwise causing financial loss to that member of the armed services in an

---

491 NY State Technology Law § 208.

492 N.Y.C. Administrative Code § 20-117.

493 For additional information, *see* http://www.nyc.gov/portal/site/nycgov/?front_door=true.

aggregate amount that exceeds $500.[494]

2. No Adverse Credit Action

A person or business who knows that a consumer is a victim of identity theft is prohibited from taking adverse action against a person's credit such as denying them credit or raising the cost of credit solely because the consumer is a victim of identity theft. Actions taken by a creditor to assist a consumer regarding his or her credit report, credit score or credit history or to limit credit or financial losses to the consumer, including the cancellation, monitoring or restructuring of consumer credit accounts, will not be considered violations of this section. A person is the victim of identity theft if he or she possesses a valid police report alleging that he or she is the victim of an identity theft crime. This provision has no section on enforcement.[495]

3. Debt Collection Efforts May Be Halted

A debt collector must cease all efforts to collect a debt from a victim of identity theft. The purported victim must provide the debt collector with a copy of a valid police report alleging that the consumer is a victim of identity theft. The identity theft must relate to the specific debt sought to be collected by the debt collector. The debtor must also provide a written statement claiming to be a victim of identify theft that relates to the allegedly due debt. This written statement can consist of the signed FTC form of ID theft victim affidavit.[496] Alternatively, the alleged debtor may submit a detailed written statement explaining why the alleged debt is not owed together with additional information set forth in the statute. This statement must then be signed by the alleged debtor specifically certifying the truth of the representations.[497] Upon receipt of this statement and required information, the principal creditor is obligated to review

494 NY Penal Law § 190.80-a (L. 2008, Ch. 226, eff. 11.04.08).

495 NY GBL § 399-e (L. 2008 Ch. 628, eff. 9.25.08).

496 http:/www.ftc.gov.

497 The certification must state: "I certify the representations made are true, correct and contain no material omissions of fact."

that information together with any other information it its files. The principal creditor may recommence debt collection activities only upon making a good faith determination that the information fails to establish that the alleged debtor was a victim of identity theft. The principal creditor must notify the alleged debtor of its decision before recommencing any collection proceedings. If the creditor ceases collection activities based on the debtor's claim of identity theft, it has an affirmative obligation to notify the credit reporting agencies of its decision and to ask for any prior adverse information on the alleged debtor because of the alleged debt to be eliminated. Any alleged debtor who knowingly submits false information to cause the debt collection efforts to cease is guilty of a misdemeanor. The Attorney General has the authority to enforce this statute and a court may impose a civil penalty of not less than $500 nor more than $1,000 per violation.[498]

J. Impact of Bankruptcy on Privacy Obligations of a Business

The questions that arise at the intersection of business bankruptcies and privacy obligations have only been addressed in the context of businesses that (1) have implemented a privacy policy and (2) possess consumer information as one of their assets. The Bankruptcy Abuse Prevention and Consumer Protection Act ("BAPCPA"), effective as of October 17, 2005, amended the Bankruptcy Code (the "Code") to address this issue largely in response to the surge in Internet companies with sophisticated mechanisms for culling detailed consumer information.

1. Bankruptcy Code Provisions Addressing Consumer Privacy

Under Section 363(b)(1) of the Code, if a debtor "in connection with offering a product or a service discloses to an individual a policy prohibiting the transfer of personally identifiable information about individuals to persons that are not affiliated with the debtor," then the trustee may only sell or lease that personally identifiable information if doing so is either: (1) consistent

[498] NY Gen Bus. § 604 *et seq.* (L. 2008, Ch.456 (A 8152 s 7297), eff. 9/1/08).

with the terms of the privacy policy or (2) approved by the court after notice and a hearing and appointment of a consumer privacy ombudsman ("CPO"). The sale or lease must also comply with any applicable non-bankruptcy laws, such as the Gramm-Leach-Bliley Act and the Federal Trade Commission Act.[499]

Section 332 of the Code provides that if a hearing regarding the sale of consumer information is required, the court will order the United States Trustee to appoint a disinterested person to serve as the CPO.[500] The role of the CPO is to provide information to the court to assist the court's consideration of the "facts, circumstances, and conditions of the proposed sale or lease of personally identifiable information under section 363(b)(1)(B)."[501]

2. Responsible Parties

Pursuant to the Code, much of the burden of protecting consumer privacy when a business files for bankruptcy falls on the trustee and, if one is appointed, the CPO. A trustee will bear the initial responsibility of interpreting any existing privacy policy of the debtor to determine whether a sale of consumer information is consistent with that policy. In the event a CPO is appointed, he or she will have significant involvement in helping the court to understand and weigh the advantages and disadvantages of a sale or lease of the consumer information.

J. Conclusion

The federal and state laws outlined above underscore the truthfulness of the old adage "no man is an island." Although that phrase may have been meant to be used in the context of demonstrating how we need to be able to count on the support of others – and they on us – it is equally accurate to note that in today's electronic database world no one should reasonably expect to live in isolation and maintain one's privacy.

---

499 *See* 11 U.S.C. § 363(b)(1)(B)(ii).

500 11 U.S.C. § 332 (a).

501 11 U.S.C. § 332 (b).

While employers, creditors and government agencies have long been asking applicants for personal information – including a Social Security number – it was not until the last decade that the government thought it was appropriate to restrain private companies from sharing that information for their own purposes, thus recognizing that the *individual* should have a say in whether or not the personal information he or she entrusted to creditor or retailer "A" can be sold to a third party or provided to an affiliate of "A" for the profit and well-being of "A." It was not until 1999 that the federal government established a federal standard for privacy in connection with individuals that provide personal information to a financial service business. Since then, we have seen too many cases of businesses losing the personal records of their customers – thereby exposing those customers to the dangers of having their identity stolen resulting in a potential loss of the customer's credit rating and sometimes obligating the customer to fight with debt collectors who allege that customers made a purchase or a financial commitment which in fact they did not.

Businesses would prefer to have a single federal standard as they find the patchwork quilt of state and municipal security breach laws a heavy compliance burden because each law has unique notification requirements. It is unclear whether we will have a single federal standard in the near future.

What is clear is that an individual's privacy is almost impossible to maintain even for the person who has minimal transactions with third parties (*e.g.*, an employer, bank, retailer or the government), as each of these entities collects and stores personal information. Therefore, even the individual who refuses to engage in "online" transactions out of a concern about "hackers" and a loss of privacy on the Internet is still at "risk" because it is likely that their bank, retailer, employer and/or their government agency will store that individual's personal information on an

electronic database that may be vulnerable to attack from unauthorized hackers. In addition, as described above, a creditor or financial institution may also report this information to a credit bureau and share the information with affiliates or third parties as described in its policy notice. Aside from Internet issues, there is always the concern of the dishonest employee who steals paper or electronic tapes containing individual account information; the “dumpster diver” who collects personal information from places where personal records are dumped and the business which goes out of business leaving its personal customer records unprotected. Therefore, it is increasingly important for every individual to be vigilant with respect to who they entrust their personal information, to monitor their own statements and credit reports to look for unknown transactions and to report any to the proper authorities.

VI. PRIVACY CONCERNS IN FEDERAL AND STATE CIVIL COMMERCIAL LITIGATION

Having addressed the myriad of regulations impacting privacy issues in different contexts, this section of the Report briefly identifies some potential problems that may arise when balancing privacy concerns with discovery obligations in civil litigation. The current state of the law poses a "Catch-22" for lawyers and litigants who need to effectively respond to discovery requests and produce all "relevant" information in civil litigation while balancing competing privacy concerns.[502] A confidentiality stipulation alone may not always be sufficient protection unless it is "So Ordered" by the court, and even then may be breached. Today's exceedingly broad disclosure requirements, particularly in federal court, combined with the requirement to engage in "e-discovery," means that privacy concerns are necessarily raised and must be addressed each and every time a lawyer, a law firm, or clients receive a request to produce information. This raises many concerns: what obstacles do the lawyer or litigant face (and what are the consequences) if the requested information is subject to privacy restrictions but produced? What rules govern discovery when the requested information is subject (or potentially subject) to a claim of privacy? Since the answer is not clear-cut, the best practice when responding to requests that implicate private or personal information is to ideally obtain a court order. This section seeks to address some issues that lawyers should be aware of when

---

[502] For a discussion of some of the issues relating to requests for information from government or quasi-government agencies that may implicate an additional set of privacy-related concerns such as state and federal constitutional protections, see the discussion herein on criminal law in Section II, *infra*. In addition, it should be noted that the Stored Communications Act, Title II of the ECPA, addresses circumstances under which a government entity can compel disclosure of information in or related to wire or electronic communications stored with an electronic communication system provider. *See* 18 U.S.C. § 2703. A government entity can compel disclosure of the content of electronic communications (*i.e.*, e-mail) only by obtaining a warrant based on probable cause for "current" data or communications that have been stored less than thirty days. Older information can only be obtained by: (1) warrant with no notice requirement to the subscriber or customer; or (2) notice to the customer or subscriber and an administrative subpoena or court order based on reasonable grounds (18 U.S.C. § 2703(d)); or (3) consent. For a more detailed discussion on this topic, *see* R. Nimmer at al, THE LAW OF ELECTRONIC COMMERCIAL TRANSACTIONS, ¶12.15[2][c].

advising their clients.

A. General Discovery Obligations

No private individual or entity enjoys total immunity from receiving or responding to a discovery request, and today, it is more likely than ever that individuals and companies will at some point be required to do so. The best practice is to create, implement, and follow a plan, policy, and protocol for uniformly responding to all discovery requests. This is even more imperative for businesses that are more likely to be a routine recipient of discovery requests because the business model is, by its nature, a repository of information (such as Google, Yahoo, Amazon, or eBay).[503]

The U.S. federal and state courts place broad discovery obligations on all litigants, whether domestic and foreign.[504] These broad obligations include the production of Electronically Stored Information ("ESI").[505] Most private and personal information responsive

---

503 *See, e.g.*, J. Markoff, *You're Leaving A Digital Trail - Should You Care?* New York Times, November 30, 2008, Business Section; M. Richtel, *What's Obscene? Defendant Says Google Offers a Gauge*, New York Times, June 24, 2008; A. Barnard, New York Investigating Facebook's Safety Rules, 9/25/07 NYTB3, 2007 WLNR 18765698. New York Times, September 25, 2007, Section C15 (New York Attorney General issued a subpoena to online social networking site Facebook as part of an investigation into whether it is misleading users by claiming it is a place where children are safe from adult sexual predators); M. Herft, *Google Adds Safeguards on Privacy for Searchers*, New York Times, March 15, 2007 (noting, among other things, that Google was the only major search engine to resist a Justice Department subpoena for vast amount of search data in 2006); M. Herft, *Google Changes Policy on Search Records*, New York Times, March 14, 2007.

504 Although as a practical matter a Court may be more sympathetic toward the burden imposed on a third-party subpoena recipient, a Court may be less sympathetic toward a litigant (especially a plaintiff who initiated the action) who claims that discovery is overly burdensome and seeks protection from searching its own records. This has greater ramifications where foreign laws are implicated, as discussed in greater detail below.

505 Fed. Civ. P. 34(a). In New York State, Article 31 of the CPLR governs pre-trial discovery but does not contain any specific provisions on electronic discovery. *See* R. Haig, Commercial Litigation in New York State Courts, 3 N.Y. Prac., Com. Litig. In New York State Courts § 23:4 (2d ed. Sept 2008). Indeed, as of August 2004, one Court noted that "[e]lectronic discovery raises a series of issues that were never envisioned by the drafters of the CPLR. Neither the parties nor the Court have been able to find any cases decided by the New York State Courts dealing with the issue of electronic discovery." *Lipco Elec. Corp. v. ASG Consulting Corp.*, 4 Misc. 3d 1019(A), 798 N.Y.S. 2d 345 (N.Y. Sup. 2004). However, despite the absence of any specific CPLR provisions governing electronic disclosure, the conference of Chief Justices implemented guidelines to the trial courts for addressing electronic discovery issues. *See* R. Haig, *supra*, at

to a discovery request today is likely to be found in the form of ESI, including but not limited to e-mail communications, electronically stored customer records, and the like. This requirement in U.S. litigation can directly conflict with foreign laws that are more protective of data and to which a U.S. litigant may be subject. When a foreign company is involved in litigation in the U.S. and subject to broad discovery, regardless of whether it initiated the litigation as a plaintiff or is defending as a party or third-party, it must balance its broad U.S. discovery obligations to produce an increasingly limitless universe of information against the competing obligation to abide by the privacy laws of its home country or the country where its information is stored. This presents a minefield of challenges for client and attorney alike. A party or non-party must produce material (including ESI) in its "possession, custody, or control,"[506] has and there may be "control" over data even though the "possession" and "custody" is in a foreign country.[507]

Although courts have occasionally contemplated that courts should not or could not compel the discovery if the entities' parent company and not the entity at issue owns the

---

§ 23.4, n.4, *citing* Conference of Chief Justices, Guidelines for State Trial Courts Regarding Discovery of Electronically-Store Information (approved Aug. 2006), available at http://www.ncsonline.org/images/EDiscCCJGuidelinesFinal.pdf, last visited as of the writing of this Report. Section 202.70 of the Rules of the Commercial Division of the New York State Supreme Court, Rule 8(b) ("Consultation Prior to Preliminary and Compliance Conferences") sets forth counsel's obligation to confer before the preliminary conference about anticipated electronic discovery issues. The Rule lists specific subjects to be discussed.

506 Fed. Civ. P. 34(a), 45(a).

507 The "possession, custody, and control" element is broadly interpreted. *See, e.g., Camden Iron & Metal, Inc. v. Marubeni Am. Corp.*, 138 F.R.D. 438, 441 (D.N.J. 1991) (citing *Scott v. Arex*, Inc., 124 F.R.D. 39, 41 (D. Conn. 1989)) (subsidiary controlled parent's documents where parent 'engineered' transaction at issue and subsidiary obtained documents about transaction from parent in ordinary course of business); *IDT Corp. v. Telefonica*, 2003 WL 230894 (S.D.N.Y. Jan. 3, 2003) (company's U.S. office compelled to produce discovery materials located in Spanish office in its control where company operated "seamlessly" in all of its locations). Failure to comply with the discovery obligation carries serious penalties. *See Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004); *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003), *Zubulake v. UBS Warburg, LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309 (S.D.N.Y.2003); *Qualcomm v. Broadcom, Inc.*, 2008 WL 66932 (S.D.Cal. 2008), *vacated in part by* 2008 WL 638108 (S.D. Cal. 2008); *Qualcomm v. Broadcom, Inc.*, 2008 WL 4858685 (S.D.Cal. 2008); *see also* CPLR 3126; *see also* R. Haig, 4 N.Y. Prac., Com. Litig. in New York State Courts § 52:24 (2d ed.) and cases cited therein.

offshore-stored ESI,[508] they have also not hesitated to require it to do so, even in the absence of traditional "veil piercing" concepts.[509] Foreign offices of the same company are not immune from production obligations,[510] and offshore material is often considered in the "control" of the U.S. company if the U.S. company and its employees regularly access the material in the course of business or employment.[511]

It cannot be assumed that a U.S. court will automatically be sympathetic to the argument that disclosure in the U.S. will cause a company or individual to run afoul of privacy laws in a foreign country, or that a court will modify or limit the broad scope of disclosure based on foreign laws. In fact, most courts have rejected the argument that production in discovery in the U.S. will subject a litigant to penalties someplace else and have refused to abrogate the litigant's existing discovery obligations.[512]

New York State offers various techniques to protect confidential information in filings such as for the filing under seal, discovery, protective orders, and confidentiality agreements and orders. For example, Part 216.1 of the New York Uniform Rules for Trial Courts will order a sealing order upon a written finding of good cause.[513] The parties may also, pursuant to CPLR

---

508 *See, e.g., Camden*, 138 F.R.D. at 441-442 (*citing Gerling Intern. Ins. Co. v. C.I.R.*, 839 F.2d 131, 140 (3rd Cir. 1988).

509 *See Camden Iron & Metal, Inc. v. Marubeni Am. Corp.*, 138 F.R.D. 438, 441 (D.N.J. 1991) (*citing Scott v. Arex, Inc.*, 124 F.R.D. 39, 41 (D. Conn. 1989)) (subsidiary had control over parent's documents where parent was engineering transaction at issue and subsidiary obtained documents regarding transaction from parent in the ordinary course of business).

510 *See, e.g., IDT Corp., supra*, 2003 WL 230894 (S.D.N.Y. Jan. 3, 2003) (company's U.S. office compelled to disclose discovery materials located in Spanish office).

511 *In re Flag Telecom Holdings*, 236 F.R.D. 177 (S.D.N.Y. 2006) (control found where employees given access to use documents in course of employment to do their jobs sufficient to permit discovery of foreign documents).

512 *See, e.g., Columbia Pictures Ind. v. Bunnell*, No. CV 06-1093 (FMC) (JCX), 2007 WL 2080419 (C.D. Cal. May 29, 2007) (ordering production of data on server located in the Netherlands even though disclosure would cause violation of Dutch law); *but see Volkswagen v. Valdez*, 909 S.W.2d 900 (Tex. 1995) (Volkswagen not required to produce corporate telephone directory in violation of Germany's data protection laws).

513 *See also Danco Labs v. Chemical Works of Gedeon Richter*, 274 A.D.2d 1 (1st Dep't 2000) (discussing the good faith standard, and the weighing of public and private interests with respect to a motion to seal court records).

Section 3103, file a protective order covering documents produced in discovery. Although usually granted, the court may balance the public and private interests in the information in deciding whether to enter the stipulated protective order.[514]

In federal court, FRCP Section 5.2 governs the filing of protected material with a federal court. The rule specifically requires that certain private information such as Social Security numbers be redacted from documents before filing. The rule further provides for the filing of motions under seal. FRCP Section 26 governs protective orders in federal courts. The court may for good cause issue a protective order under certain circumstances. A party moving for a protective order must confer with the party seeking the documents before making a motion to the court. The court may for good cause issue an order to prevent discovery of certain confidential information or trade secret. The court may also allow such information to only be revealed in a limited way (*e.g.*, outside counsel and experts). FRCP Section 37 specifically discusses the costs of failed motions for protective orders, where there is a failure to confer, or where a request to bar discovery of certain information is unreasonable.

B. Preparing to Respond to the Request

Notwithstanding the obligations to search for and produce all "relevant" information, a discovery respondent must still comply with privacy regulations. In advising their clients, lawyers should seek to answer the following questions in order to determine how to proceed.

1. Who is the Request Directed to?

As noted throughout this Report, different regulations will apply depending on who is being asked for the information and what kind of information is being requested. An individual

[514] *See* R. Haig, Commercial Litigation in New York State Courts (2008) § 20:23 and § 20:30. For a form Confidentiality Agreement often used in the Commercial Division of the Supreme Court of the State of New York *see* Stipulation and Order for the Production and Exchange of Confidential Information created by the New York City Bar Association's Committee on State Courts of Superior Jurisdiction available at http://www.NYC.bar.org/publications/reports/.

being asked to search his or her own personal e-mails (or even his or her e-mails at work), may be less successful at overcoming the obligation to produce because that individual retains the power to waive his or her personal privacy interests in the information such as e-mails. If the recipient of the request is a "financial institution," in which case the obligations are impacted by GLB (*see* Section V., *supra)* the FTC's "Privacy of Consumer Financial Information" regulations[515] and other regulations promulgated by various federal agencies that regulate specific types of financial institutions.[516] If the recipient is a "covered entity," then the HIPAA,[517] applies. If the recipient is a company that provides telephone and Internet communications, and possesses user/subscriber information, the disclosure obligations are impacted by ECPA (including the "Wiretap Act"[518] and the "Stored Communications Act").[519] The subpoena provisions of the DMCA[520] may also impact disclosure since it can be construed to apply to anyone engaging in electronic communications or handling electronic material. The DMCA will most certainly apply if the recipient (*i.e.*, an ISP) possesses identifying information regarding alleged copyright infringers.[521]

2. What Kind of Information is Requested?

As discussed herein, the type of information requested and within the request recipient's

---

515 16 C.F.R. Part 313.

516 *See* Section V, herein.

517 Public Law No. 104-191. *See* Section III, herein.

518 18 U.S.C. § 2510 *et seq*. *See also* Section I.A.3, herein.

519 18 U.S.C. § 2701 *et seq*. Disclosure of the content of a communication might violate the ECPA, while disclosure of subscriber records, might not (names, addresses, and phone numbers of parties called by subscriber not "contents" of communication); *See* 18 U.S.C. § 2702(c); *see Hill v. MCI Worldcom Comm.*, 120 F. Supp. 2d 1194 (S.D. Iowa 2000); *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105 (E.D. Mich. 1998).

520 17 U.S.C. § 512(h), *see* Section I.B.3 herein.

521 *But see Recording Ind. Ass'n of Am. v. Verizon Internet Servs., Inc.*, 351 F. 3d 129 (D.C. Cir. 2003), (under the DMCA a subpoena may only be issued to an ISP engaged in storing on its servers material that is infringing, and not to an ISP acting as a conduit between two Internet users). *cert denied*, 125 S. Ct. 309, 160 L.Ed.2d 222 (2004); *In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771 (8th Cir. 2005). *See* Section I, herein.

custody, control, or possession will dictate the controlling regulations.[522]

3. How is the Request Made?

There is no obligation to disclose information in response to a request (*i.e.*, oral or letter) and attorneys should not do so where private information is involved. In some circumstances, a subpoena or document request may not itself be sufficient protection against an unauthorized disclosure of private information.[523] The best protection under any set of circumstances is insisting on the issuance of a court order or a stipulation to be "So Ordered" by the Court, or moving for a protective order or moving to quash a subpoena if the requesting party refuses to seek a court order. When dealing with information kept in a non-U.S. jurisdiction, the best method is to proceed pursuant to the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, which requires that a "judicial authority" (usually a U.S. judge) issue a Letter of Request to the Central Authority established by the country from whom discovery is sought to be obtained.[524]

4. Where is the Information Kept?

The final question in the analysis will determine whether the recipient is bound not only by U.S. privacy regulations but also the privacy regulations of foreign countries. The

---

522 *See* Section I and IV (identifying personal information, such as names, physical addresses, phone numbers, Social Security numbers, account numbers or IP addresses); Section V (financial information such as financial account numbers, credit card numbers, financial data, passwords, or credit information); Section I (User or subscriber information such as "Google" searches, purchasing behavior, "Cookies," or web sites visited); Sections III and IV (medical records or employment records); and Section I (contents of electronic communications such as e-mail, texts, instant messages, etc. that contain any of the above).

523 *See, e.g.*, DMCA 17 U.S.C. § 512(h) (permitting copyright owners to subpoena a service provider for information to indentify an alleged infringer); GLB (allowing certain information in response to subpoena); 18 U.S.C. § 2701 *et seq.* (ECPA does not provide authority for the disclosure of the contents of communications in response to a request or subpoena issued by a private party in a civil proceeding); *O'Brady v. Superior Court*, 139 Cal. App. 4th 1423 (2006) (Court held that enforcement of subpoena would violate the ECPA). Although at least one federal court has held that a service provider was not liable under ECPA for disclosing electronic communications in "good faith reliance" on a civil subpoena (*Kenneth A. McCreedy v. eBay, Inc.* 435 F. 3d 882, 891-92 (7th Cir. 2006)). That holding relied on statutory provisions that only permitted disclosure in response to a "grand jury subpoena." (*See also* 18 U.S.C. § 2520(d) and 2702(e)).

524 *See* Hague Convention Article 2.

ramifications of dealing with information stored in a non-U.S. country are briefly discussed below.[525]

C. Methods of Permissible Disclosure

Assuming a client possesses responsive (and non-privileged) information to be produced, there are four generally applicable advisable methods to use in order to protect against liability from the disclosure of personal or private information, as mentioned in other areas of this Report: Consent, Notice, Legal Process, and Policies and Procedures.[526]

1. Consent

Consent is one of the best defenses to an allegation of unauthorized disclosure of private information. Although the simplest method of obtaining consent is directly contacting the individual in question, this is not always practical when the privacy rights of hundreds, if not thousands, of people may potentially be impacted. User agreements, Terms of Use, employment agreements or handbooks, or contracts may all have provisions for consents to disclosures, and these types of documents should always be consulted to determine whether such consent exists.[527]

2. Notice

Notice to potentially affected individuals will also help defend against allegations of unauthorized disclosure, even if notice is not specifically required by applicable statute.[528]

3. Policies and Procedures

A company is best served by creating, implementing, and following a set of rules and policies that include responding to discovery requests. If the responding party already has

---

525 *See* Section IV D, herein.

526 *See* discussions at I-V, *supra.*

527 *See* Section I, *supra.*

528 *See, e.g., Polito v. AOL Time Warner, Inc.*, Civ. No. A03-CV-3218, 2004 WL 3768897 (Pa. Jan. 28, 2004).

contractual agreements, "Terms and Conditions" on its web site or sent to customers, terms of service, and/or privacy policies that can be construed as "agreements" regarding how private information may be handled and disclosed, it is imperative that these agreements be followed. A breach (or even perceived breach) of these policies could result in an FTC action (which are rare) or a class action (which is more likely given the prominence of class action lawsuits).[529]

There are regulations that require the government to compensate a party that is providing routine facilities for the interception and disclosure of information (such as YouTube, Google, Yahoo, and the like, which may be the subject of regular and routine subpoenas). Rule 26(b)(1) and its state corollary, CPLR Section 3103(a), permit cost-shifting. Depending on the court, the nature of the litigation, and the degree to which the client can afford the expense, when a party imposes an exceptionally burdensome discovery request, a client will be forced to expend significant costs (including legal fees) in order to limit the discovery and, even then, may still have to produce certain personal information.

D. Foreign Privacy Laws

1. Discovery and ESI Obligations of Foreign Litigants in the U.S.

Privacy laws of foreign countries protect consumer and employee e-mails and prevent corporations from using information that derives from or is stored in a jurisdiction with greater restrictions and privacy protections than the U.S. Often the privacy laws of other countries are much more stringent than those in the U.S. Many foreign laws regulate the length of time and for what purpose data can be retained at all. In addition, most other countries do not permit as broad discovery as the U.S. Courts have been increasingly willing to do. The obligation to turn over broad range of discovery in the U.S. must be balanced with a foreign litigant's privacy

[529] *See* Section I, *supra*.

obligations under the laws of its home or other foreign countries. [530]

Foreign privacy laws may interfere with the ability of a company to preserve ESI, transmit it to the U.S., and/or produce it in a U.S. litigation because of data protection laws and blocking statutes that complicate the process, discussed more fully below.

a. Data Protection Laws

Various data protection and privacy laws exist in Europe and other countries.[531] Such data protection statutes may prevent private information from being stored longer than necessary or used for any purpose other than the one for which it was collected.[532] These statutes may similarly prevent transmission or disclosure to the United States.[533] The 1995 EU Directive expressly allows EU member states to state that the transfer of data is permitted if it is

---

530 For an excellent discussion of the practical challenges of seeking discovery pursuant to the Hague Convention, and the protections a country will afford to its own citizens' information, *see* G. Adler *et al*., Electronic Discovery and the Global Workplace, PLI, October 29, 2008, at n. 28-29 (*citing* Restatement (Third) of Foreign Relations Law of the United States 473 Reporter's Note 4 (2008) (*citing* Corning Glass Works v. International Telephone and Telegraph Corp., OLG Munchen, 10/31/80; 11/27/80, 1981 Juristenzeitung 538, 540, reproduced in English in 20 Int'l Leg. Mat. 1049, 1025 (1981)) (indicating that the German court, in a pre-ESI decision concerning a Letter of Request sent to Germany, strictly construed Article 23 of the Hague Convention and denied the request for documents); and *Metso Minerals Inc. v. Powerscreen Intern. Distribution Ltd*., No. CV 06-1446 (ADS) (ETB), 2008 WL 719243, at *1 (E.D.N.Y. Mar. 18, 2008) (chastising a party for ignoring the court's warning as to the limitations in the U.K. on pre-trial discovery and issuing requests that were "overly broad and blatantly inconsistent with U.K. precedents governing pre-trial discovery under Hague Convention on Evidence.").

531 *See* 1995 EU Data Protection Directive and various data protection and privacy laws that exist in each of the individual EU Member States, all of which are available at http://en.wikipedia.org/wiki/List_of_European_Union_directives and http://eur-lex.europa.eu/en/index.htm; *see also* G. Adler *et al*., *Electronic Discovery and the Global Workplace*, PLI, October 29, 2008 at 3, *citing, inter alia*, EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data; see also EU Directive 2002/58/EC on Privacy and Electronic Communications (currently under review). To date the twenty-seven EU member states are Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom. Source: http://europea.eu/abc/european_countries/index_en.htm (last visited Dec. 12, 2008).

532 G. Adler *et al*., *Electronic Discovery and the Global Workplace*, PLI, October 29, 2008, at fn. 37, *citing* EU Data Protection Directive, Articles 6 and 25.

533 *Id*.

"necessary for the establishment, exercise or defence of legal claims."[534] However, commentary on this issue has noted that this either is not intended to or will not be interpreted by member states to mean "legal claims" in U.S. litigation as many member states lack pre-trial discovery as conducted in the U.S.[535]

b. Blocking Statutes

In 1987, in *Societe Nationale Industrielle Aerospatiale v. United States District Court*, the U.S. Supreme Court held in a case involving a French party that the Hague Convention does not pre-empt the obligations imposed by the FRCP.[536] In response, many foreign countries (including Australia, Canada, France, Japan, the Netherlands, Sweden, and the United Kingdom) enacted so-called "blocking" statutes to protect their citizens against the American's increasingly broad discovery practices.[537] These blocking statutes forbid the transfer of data or information for certain purposes (including responses to U.S. discovery requests or orders).[538] Criminal penalties or prosecution in the home country may result, even if the party produces the information voluntarily.[539] These blocking statutes reflect a visceral reaction on the part of foreign countries who view the uninhibited disclosure of all information as antithetical to their laws and culture.[540]

---

534 *Id*. at fn. 39, *citing* EU Data Protection Directive, Articles 8.

535 *Id*. at n. 38 and 40, *citing* German Federal Data Protection Act Section 4(c)(1)(3); Spies/Schroeder, Auswirkungen der elektronischen Beweiserhebung (eDiscovery) in den USA auf deutsche Unternehmen, Multi-Media Recht (MMR) 2008, 275 (279). The Adler article notes that the French Data Protection Agency ("CNiL") investigated document requests in U.S. discovery, and indicates that the U.S. Department of Commerce is engaged in continuing discussions with the EU to address these continuing conflicts. Adler at n. 38. It is not clear whether and how the evolution of these discussions will change with the new administration and presumed nominee for Secretary of Commerce.

536 482 U.S. 522 (1987).

537 *See* M. Gottridge and T. Rouhette, *'Blocking' Statutes Bring Discovery Woes*, April 30, 2008, the New York Law Journal at n. 3.

538 *Id*.

539 *Id*.

540 *See id*., *citing* P. Murray, "Taking Evidence Abroad: Understanding American Exceptionalism," 10 Zeitschrift fuer Zivilprocess International 343 (2005); L. Minch, "U.S. Obligations Under the

In its thirty-year history since its enactment, the French blocking statute had never been prosecuted or enforced.[541] Accordingly, the U.S. courts tended to not take it seriously and declined to modify a French party or non-party's discovery obligations based on a threat of prosecution under the French blocking statute.[542] On the other hand, some U.S. Courts have in the past directed litigants to the procedures under the Hague Convention to determine the issue.[543]

That decades-old history of non-prosecution came to an abrupt halt a year ago when the French Supreme Court affirmed a criminal conviction of a U.S. lawyer and fined him 10,000 euros for seeking discovery from a French entity in connection with U.S. litigation without submitting to the process dictated by the Hague Convention.[544] Although this case far from resolves the issue, now that the threat of actual prosecution under the French blocking statute is

---

Hague Evidence Convention: More Than Mere Goodwill?," 22 Int'l Law. 511, 512 (1988). France's blocking statute is generally seen as the most extreme and restrictive and states: Subject to treaties or international agreements and applicable laws and regulations, it is prohibited for any party to request, seek or disclose, in writing, orally or otherwise, economic, commercial, industrial, financial or technical documents or information leading to the constitution of evidence with a view to foreign judicial or administrative proceedings or in connection therewith." *Aerospatiale*, 482 U.S. at 526 n. 6 (quoting French Penal Code Law No. 80-538, Article 1A). The disclosure is prohibited when it is likely to affect "French sovereignty, security, or 'fundamental economic interests.'" Gottridge, *supra*, at 1 n. 4, *citing* French Penal Code Law No. 80-538 at p. 1799.

541 *See* Gottridge, *supra*.

542 *See U.S. v. Gonzalez*, 748 F.2d 74, 77-78 (2d Cir. 1984); *Graco, Inc. v. Kremlin, Inc*., 101 F.R.D. 503, 508 (N.D. Ill. 1984); *Adidas (Canada) Ltd. v. SS Seatrain Bennington*, No. 80 Civ. 1911 (PNL), 1984 WL 423, at *3 (S.D.N.Y. May 30, 1984) (Leval, J.); *In re Vivendi Universal, S.A. Secs. Litig.*, No. 02 CV 5571 (RJH) (HBP), 2006 WL 3378115 at *2-3 (S.D.N.Y. Nov. 16, 2006); *Bodner v. Banque Paribas*, 202 F.R.D. 370 (E.D.N.Y. 2000); *Strauss v. Credit Lyonnais*, 242 F.R.D. 199 (E.D.N.Y. 2007); *see also First Am*., 154 F.3d at 21 (U.K. laws of confidentiality); *Remington Prods. Inc. v. N. Am. Philips Corp.*, 107 F.R.D. 642 (D. Conn. 1985) (Netherlands blocking statute had never been enforced).

543 *See In re Perrier Bottled Water Litigation*, 138 F.R.D. 348, 355 (D. Conn. 1991) (*citing* the French blocking statute); *Hudson v. Hermann Pfauter GmbH & Co.*, 117 F.R.D. 33, 38 (N.D.N.Y. 1987); *see also Deman v. Terrien*, No. B148080, 2002 WL 1824941 at 5 (Cal. Ct. App. Aug. 8, 2002) (unpublished).

544 Gottridge, *supra*, at n. 14, *citing* Cour de Cassation Chambre Criminelle [Cass. Crim.], Paris, Dec. 12, 2007, Juris-Data no. 2007-332254; *see also* D. Schimmel and E. Rosenfeld, New Respect for Hague Evidence Convention in Discovery, 239 N.Y.L.J. 4 (2008); *but see* Gottridge, *supra*, at n. 17, *citing* Cour d'Appel Paris, 1e ch., Dec. 18, 2003, RG No. 2002/18509 (granting request for documents because requests sufficiently limited to precise time period).

evidenced, French parties and non-parties alike (as well as parties from other countries with blocking statutes) may find better ground to object to U.S. discovery requests in general, but particularly with respect to otherwise private information.

E. Conclusion

Privacy regulations seeking to protect private information are often at odds with the policy driving broad disclosure in litigation. Lawyers must be mindful of this conflict and seek to balance these competing interest when advising their clients. Further study is warranted to determine whether a change in the law is necessary to assist lawyers in navigating this difficult situation, including but not limited to whether New York State should adopt regulations and/or additional guidelines to address electronic discovery in general and also to govern discovery of private information subject to existing regulations.[545]

[545] For more detail on this topic *See* A. Serwin, Information Security and Privacy: A Practical Guide to Federal, State, and International Law, § 31-71 (2008); D. Garrett, Conducting E-Discovery in Europe: Practice Pointers for Corporate Counsel, PLI Publications (2008); J. Chadwick, Privacy Issues in Litigation: Responding to Private Litigants' Requests for Personal Information, PLI Publications (2008).

VII. REPORT CONCLUSIONS

The mission of the Task Force was to identify certain privacy issues impacting lawyers and their clients (both businesses and individuals) in the areas of health, criminal, employment, litigation, business, and intellectual property. As it embarked on fulfilling its mission and began identifying issues for further exploration and study, the Task Force quickly realized that privacy has become an enormous area of law that encompasses nearly all practices of the law. As the Task Force continued its research and analysis, its members indicated the enormity of the task, and expressed concern that a complete and total assessment of all aspects of privacy law was difficult, if not impossible. The Task Force therefore focused on what its members identified as some of the most important issues facing lawyers and clients today. As was its mission, the Report has identified certain areas that the Task Force may evaluate for further study, analysis, and/or proposals for advocating a change in the law or an implementation of additional laws in the privacy arena if ultimately determined to be warranted. The Report has further provided opportunities to educate the legal profession (and thereby the public) on the current state of the law on select key privacy issues. Where possible, the Report has also evaluated the available remedies for violation of the privacy laws addressed. In doing so, this Report attempts to answer the fundamental question of what rights exist to protect personal and private data, and what obligations individuals and businesses have when accessing and using certain information.

An individual's privacy is nearly impossible to maintain due to all the entities in basic daily life that collect, use and store personal information. Health and financial records are of great concern, and technology has made their accessibility and dissemination much easier – this leads to an increased need for scrutiny and enforcement. Technological protections of privacy are available, although not fool-proof and not easy for the average individual to keep up with.

In litigation, personal information is divulged both voluntarily (*e.g.*, in allegations set

forth in a complaint or an administrative charge) and involuntarily (*e.g.*, in employment litigation, such as where: (i) plaintiff employees routinely seek personal information concerning co-workers and/or details concerning sexual harassment complaints asserted by other workers that is claimed to be relevant to liability issues; and (ii) defendant employers regularly seek psychological and other medical information concerning plaintiffs in order to defend against emotional distress and other damages claims). Carefully crafted protective orders may be key in determining who is to be entrusted with personal information, and then monitoring where it ends up.

Some Task Force members expressed their belief that this Report was an initial step towards a more detailed and involved analysis of the important issues raised in the Report. These members emphasized that they wish to continue the process of studying these issues, collecting input from additional sources, and analyzing how the privacy laws in each area of law intersect and impact each other.

That said, in its study, the Task Force identified areas of the law where it strongly suggests the Association should continue to examine the sufficiency of the law and its enforcement, and whether legal reform is warranted, necessary, and practical, and whether the Association should advocate for such change. As was noted by Matthew Barach, the Internet and Information Privacy Counsel for the New York Consumer Protection Board, "the law has not caught up with the illicit sophisticated organizations, the speed of technology and information, and the ways in which the world is rapidly changing.[546] With respect to the data breach, the existing laws do not adequately address the fact that 'information' is more valuable to

[546] Interview between Co-Chair Alison Arden Besunder and Matthew Barach, December 22, 2008 ("interview").

the criminals the longer it is kept off the street."[547]

To that end, the Task Force members were asked to investigate whether the current laws in their particular field of law address how long private information is kept and whether advocating a change of the law in this regard is warranted.[548] The members reported back that they are not aware of any current laws addressing this specific point.

It was also recommended that the Task Force should further analyze whether there are sufficient resources available in the law for individuals to protect information commonly used as identifiers, such as Social Security numbers and driver's license numbers or whether the law should be reformed to allow consumers to obtain "ID" numbers for use in e-commerce or other daily uses (which can changed annually by the consumer, or more frequently in cases of breach or identity theft).

In the area of employment law, the Task Force was able to identify but did not have sufficient opportunity to conduct a comprehensive and exhaustive analysis of several areas of employment law that were identified by employment law members of the Task Force as raising important privacy concerns. Among those areas identified is the Family Medical Leave Act, which requires employees to disclose certain medical information concerning themselves and/or their family members as a condition of approval of a leave of absence for purposes of the employee's own medical condition or that of a family member. Moreover, in cases where there is a dispute, the employer may require the employee to undergo another examination by a health care provider selected by the employer. In addition, the Americans with Disabilities Act, as well

---

547 Since the laws are aimed at notice to the consumer, a consumer may become less vigilant as time goes on and discover that it has been the victim of identity theft several years after notice of the breach.

548 Moreover, although there has been some progress made in curtailing the use and dissemination of Social Security numbers, it has been expressed to the Task Force that to a large extent the damage may already have been done.

as the New York State Human Rights Law and the New York City Human Rights Law, all require the employer and the employee who suffers from a disability to engage in an interactive process that may include employer consultations with the employee's health care provider in order to determine what accommodations are available and most appropriate to the employee's condition that, if provided, would enable the employee to perform the essential functions of the job. The Labor and Employment Section of the Association has indicated an interest in studying these and other privacy issues discussed in the Report insofar as they arise in the workplace context. The Labor and Employment Section expressed to the Task Force Co-Chairs that it intends to do so, possibly by the appointment of a Section subcommittee appointed by the Chair of the Labor and Employment Section. The Task Force recommends that such efforts by this and other Association Sections be encouraged.

It was also suggested that the Task Force further analyze the manner in which private entities (including, but not limited to, credit bureaus) collect and use information about consumers, and whether there is sufficient regulatory oversight of such activities. This may include investigating whether and to what extent the collection of consumer information contributes to identity theft and whether additional measures could assist consumers to know what information is collected and how it is being used. This may also include investigating whether sufficient resources exist for governmental oversight of these activities, and whether a special committee or regulator ombudsman should be appointed to consider regulation reform, oversight, and implementation of penalties.

Another recommendation was that the Task Force investigate whether credit bureaus should be required to take additional steps to help consumers protect their identity. This may include whether or not credit bureaus should be subject to the same type of identity verification

in opening a credit file that financial institutions are required to do pursuant to the "Red Flags" rules discussed elsewhere in this Report.

With respect to health issues, many major companies such as Google are seeking to launch "ehealth" services. However, these companies may not necessarily be "covered entities" under HIPAA and therefore need not be HIPAA compliant. A potential breach of information in that instance could be potentially disastrous. In addition, it has been reported that President Barack Obama intends to seek digitization of all medical records. It was suggested that the Task Force continue to investigate any newly introduced administration agenda items and whether a change in the law is warranted or necessary as the policies of the new administration are implemented.

As described in this Report, the law is developing to address the challenges raised by technological advances that have caused the world to be "smaller" and privacy to be more difficult to maintain. As lawyers, our role as advisors is impacted both personally and professionally. In suggesting that the Association continue to study privacy issues, the Task Force suggests further consideration of what is meant by privacy, what needs to be protected, how that can be accomplished, and what steps will be required to do it. Having completed the first step of canvassing the state of the law and identifying some of the issues that may warrant further study, the Task Force suggests the Association proceed to the next step of exploring those issues, identifying a collective view, and outlining a plan of reform, where necessary.

It is this Task Force's conclusion that while the existing laws at the federal and state level may be sufficiently comprehensive and broad to address technological issues impacting privacy as it stands today, technology evolves quickly and the existing laws need to be constantly evaluated to ensure their sufficiency. In addition, agencies with limited resources should be

encouraged to give priority to the enforcement of existing laws. To this end, the Task Force strongly suggests that the Association continue to examine the sufficiency of the law and its enforcement, maintain oversight of the identified areas of concern, evaluate additional areas of law for examination, seek further input from local bar associations and relevant public interest groups, and update this Report regularly on an as-needed basis.

The members of the Task Force recognize that just in the time this Report was drafted, the law has changed and technology has advanced. Even in the last stages of finalizing the Report, new articles reporting on studies conducted in this field appeared on a daily basis. Some parts of this Report could therefore become dated even before the Report is distributed. Therefore, with regular updates lawyers can be provided with a resource to use both personally and professionally to help protect themselves and their clients.

Appendix to the Health Law Chapter
GLOSSARY

CMS	Centers for Medicare and Medicaid Services
CPLR	NY Civil Practice Laws and Rules
DOH	NYS Department of Health
DOJ	U.S. Department of Justice
HER	Electronic Health Records
EPHI	Electronic Protected Health Information
HEAL NY	Health Care Efficiency and Affordability Law for New Yorkers Capital Grant Program
HIE	Health Information Exchange
HIO	Health Information Organization
HIPAA	Health Insurance Portability and Accountability Act of 1996
Kennedy/Leahy Bill	Health Information Privacy and Security Act of 2007
LIPIX	Long Island Patient Information eXchange
MHL	Mental Hygiene Law
NCVHS	National Committee on Vital and Health Statistics
NHIN	Nationwide Health Information Network
NPP	Notice of Privacy Practices
NYHISPC	New York Health Information Security and Privacy Collaborative
OASAS	NYS Office of Alcoholism and Substance Abuse Services
OCA	Office of Court Administration
OCR	U.S. Department of Health & Human Services, Office of Civil Rights
OIH	U.S. Department of Health & Human Services, Office of Inspector General
OMH	NYS Office of Mental Health
OMRDD	NYS Office of Mental Retardation and Developmental Disabilities
OPMC	Office of Professional Medical Conduct
PA	Physician's Assistant
PCIP	Primary Care Information Project
PHI	Protected Health Information
PHL	Public Health Law
PRO(TECH) Act	Protecting Records, Optimizing Treatment and Easing Communication Through Healthcare Technology Act of 2008
RHIO	Regional Health Information Organizations
SA	Specialist's Assistant
THNIC	Taconic Health Information Network

NEW YORK STATE BAR ASSOCIATION
HOUSE OF DELEGATES
RESOLUTION ADOPTED APRIL 4, 2009

WHEREAS, the mission of the Privacy Task Force was to: (1) identify discrete areas of privacy for lawyers and those they represent (businesses and individuals) concerning the Internet, health and financial information; (2) review the laws, statutes and rules in these areas; (3) propose procedural and substantive changes where necessary; (4) provide opportunities to educate the profession and the public on privacy with the aim of ensuring that our laws, policies and practices are designed to reduce the risk of violations of privacy; (5) review and report on the current remedies/compensation available to those whose data have been seized for illegitimate purposes; and (6) prepare a report which covers the current state of the law and shall recommend any appropriate reforms, both by statute, policy and practice, to the Executive Committee and the House of Delegates; and

WHEREAS, the Privacy Task Force fulfilled its mission and prepared such report, inviting input from all Sections as well as from ***specialty, local, and county bar associations and privacy experts; and***

WHEREAS, the Privacy Task Force held a Privacy Summit in New York City where experts in privacy law identified some of the most pressing areas in privacy law at this time; and

NOW, THEREFORE, IT IS

RESOLVED, that the New York State Bar Association approves, with its thanks, the Report of the Privacy Task Force; and it is further

RESOLVED, that the Association endorses certain best practices set forth in the Report: (1) that web site owners should include the provisions on pages 40-43 of the Report in their Terms of Use; (2) that web site owners should include the provisions on pages 46-47 of the Report in their Privacy Policy; (3) that lawyers should take steps to avoid or mitigate the risk that client information obtained in the course of their legal practice, the privacy of which is protected by federal, state or local law, will be accessible to unauthorized persons (see pages 49-60); (4) that lawyers should treat health information obtained in the course of their legal practice with the appropriate standard of care to meet the privacy protections required by applicable law (see pages 77-125); (5) that lawyers should take reasonable steps to protect medical records and other health information obtained in the course of their legal practice from destruction or inadvertent disclosure, theft or other security breach (see pages 102-106); (6) that discovery request respondents should seek to address reasonable privacy concerns in responding to discovery requests (see pages 209-221); and (7) that agencies should strive to commit adequate resources to enforce compliance with existing privacy laws; and it is further

RESOLVED, that the Association reaffirms its commitment to the goal of providing opportunities to educate the profession and the public on privacy and suggests interdisciplinary

CLE programs be conducted to address the following areas identified by the Task Force and experts in privacy law as some of the most pressing areas in privacy law at this time:

1. Medical Information Technology: (a) agency and government enforcement of privacy regulations for compliance and funding to permit smaller organizations to become compliant without oppressive financial cost; (b) the effectiveness and enforcement of penalties for poor or breached security; (c) assistance to covered entities to implement internal controls, including education of medical personnel to ensure proper, secure, and compliant use of information systems; (d) whether there should be private rights of action for breaches of medical security; (e) whether patients should be able to opt-out of having their records in a national healthcare database and the implications of such; and (f) whether information voluntarily submitted to medical databases (e.g., Google Health) should be subject to new privacy protections and regulations that arise out of the recently enacted stimulus legislation.
2. Employment: The extent to which an employer may access and use information (both employment and non-employment related) about an employee or potential hire, including information about the individual posted on the Internet that cannot be readily verified and material posted on social networking sites.
3. Record Retention and Destruction: The disposal, destruction, and maintenance of client files (both paper and electronic) by lawyers and law firms, including whether there should be a "catch-all" period for mandatory destruction of all records containing non-public personal information of consumers;
4. Bankruptcy Issues: The ability and preconditions to sell private consumer information in bankruptcy proceedings as an asset of the bankruptcy estate (for example, when a privacy notice says that the bankrupt company doesn't share information);
5. Social Security Numbers: The use of Social Security numbers as an identifier for any purpose, with a specific focus on: (a) how to prevent future use of Social Security Numbers as common identifiers; (b) how to remedy past and present abuses; (c) what is an appropriate alternative for authenticating identity (e.g., biometric identity cards);
6. Uniformity in Breach Notification Laws: Whether there should be a national standard for data breach notification;
7. Enforcement and prosecution: How to enforce and prosecute data breaches and privacy violations such that the risk of inadequate data security and privacy violations are more than merely a "cost of doing business"; and
8. Technology Standards: Whether a baseline can be established as to the minimum level of technological protection an attorney must use in protecting client information and the attorney-client privilege;

and it is further

RESOLVED, that the officers of the Association are hereby empowered to take such other and further steps as they may deem warranted in order to implement this Resolution.