The Sedona Conference Journal

Volume 12 2011

United States Approach to Privacy Protection in Litigation

Steven C. Bennett

Recommended Citation: Steven C. Bennett, *United States Approach to Privacy Protection in Litigation*, 12 SEDONA CONF. J. 173 (2011).

UNITED STATES APPROACH TO PRIVACY PROTECTION IN LITIGATION

*By Steven C. Bennett**
Jones Day
New York, NY

OVERVIEW

The conflict between U.S. discovery rules and international data protection (and other similar) limitations does not take place in a vacuum. The U.S. approach to data privacy, although different from that of much of the rest of the world, does include constitutional, common law and statutory bases for assertions of privacy-based protection of information. Where U.S.-derived privacy concerns arise in the context of discovery requests in litigation, U.S. civil procedure rules, and case law, acknowledge the possibilities for shaping relief to accommodate legitimate privacy concerns. The means by which U.S. courts protect U.S.-derived privacy concerns may offer useful insights into the appropriate means for accommodating similar concerns, when they arise from privacy regimes outside the United States.

SOURCES OF U.S. PRIVACY LAW

The notion that individuals have a right to privacy is not a new development, yet, this is not a right expressly protected in the U.S. Constitution. Instead, the right of privacy receives protection from various sources, including scattered clauses of the Constitution and its amendments, common law and various statutes.

A. History Of The Right To Privacy

The modern American definition of privacy as the "right to be let alone" was explained at length by future Supreme Court Justice Louis Brandeis and Samuel Warren in 1890.[1] Their article, "The Right to Privacy," focused on the technological and business developments of the day, i.e., instantaneous photographs, press and newspaper enterprises, as methods by which the details of private lives could be publicly disseminated. The authors urged that the law should evolve to respond to such technological and social changes, and their article laid the groundwork for the concept of informational privacy, that is, control over information about oneself.

This "right to be let alone" gradually developed, even though no specific right to privacy is enumerated in the U.S. Constitution. The Supreme Court has construed

---

* Steven C. Bennett is a partner at Jones Day, and Chair of the Firm's Ediscovery Committee. The views expressed are solely those of the author, and should not be attributed to the author's firm, or its clients. Jordan Schneider and Patrick Leibach, summer associates at the firm, assisted in the preparation of this paper.

1 Warren & Brandeis, *The Right to Privacy*, 4 HARVARD L. REV. 193 (1890).

provisions in the Bill of Rights to provide some protection to a variety of elements of individual privacy, yet, there is simply no explicit Constitutional guarantee of a blanket "right to privacy." For example, the liberty guaranteed in the Constitution has been construed to protect a person from unwarranted government intrusion into a dwelling or other private place, and "liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct."[2]

These constitutionally-based privacy rights apply only to protect an individual from a government actor infringing upon the individual's rights.[3] They do not apply to private actors, which is why private arrangements, as well as legislation and regulations developed by the government, can become an important source of privacy protection.

B. Sources Of Privacy Protection

The development of the right to privacy can be traced through early decisions of the Supreme Court concerning "substantive due process." Throughout these cases, which explored individual rights with respect to schooling, housing, contraception, wiretapping, and marriage, the Supreme Court began to extend constitutional protection for private behaviors in certain contexts and among certain individuals. The extension of the protection of these individual rights was highly fact-intensive and piecemeal – with the Court examining the underlying facts of every case in a very detailed fashion.

1. Constitutional Right To Privacy

As discussed, the actual word "privacy" does not appear in the Constitution. However, the Supreme Court has interpreted many of the guarantees in the U.S. Constitution's Bill of Rights to create "zones" of privacy.

In an early decision on the privacy implications of wire-tapping, the Court faced the question whether the government's interception of telephone conversations and use of such conversations as evidence amounted to a violation of the Fourth and Fifth Amendments.[4] The Supreme Court ruled in favor of the government, holding that wire-tapping was not an unreasonable search and seizure within the meaning of the Fourth Amendment.[5] Although this case did not recognize a privacy right against wiretapping, the language in Justice Brandeis' dissenting opinion set the groundwork for understanding the constitutional guarantees of liberty and privacy:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[6]

---

2 *Lawrence v. Texas*, 539 U.S. 558, 562 (2003).
3 The Thirteenth Amendment prohibiting slavery is the only Amendment that regulates the conduct of an individual or private entity rather than the conduct of the government.
4 *Olmstead v. United States*, 277 U.S. 438 (1928).
5 *Id.* at 466.
6 *Olmstead*, 277 U.S. at 478 (5-4 decision) (Brandeis, J. dissenting).

The Supreme Court faced right to privacy issues in the controversial case *Roe v. Wade*, which struck down a Texas anti-abortion law, holding that a woman's right to an abortion fell within the protection afforded by the Fourteenth Amendment.[7] The Court found that "the right of privacy…is broad enough to cover the abortion decision," but that the "right is not absolute and is subject to some limitation; and that at some point, the state interests as to protection of health, medical standards, and prenatal life, become dominant."[8]

The *Roe* decision is significant in that it recognized the right of privacy as a "fundamental right," thus, any statute limiting such a fundamental right may be justified only by a "compelling state interest."[9] While the "compelling state interest" of protecting unborn human life and the health of pregnant women were claimed in *Roe*, the Court found those interests did not become a compelling interest until the end of the first trimester, when the fetus becomes "viable."[10] After that "compelling" point, a state may prohibit abortion, except in cases where abortion is necessary for the preservation of the life or health of the mother.[11]

Constitutional privacy rights have also been extended in relation to other circumstances and situations. For example, the notion of privacy under the Fourth Amendment was expanded in *Katz v. United States*, a case in which the Court held that Fourth Amendment protections against unreasonable searches and seizures required the police to obtain a search warrant in order to wiretap a public pay phone.[12] The Court held that the Fourth Amendment protected people, not just places.[13] According to the Court in *Katz*, "once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[14] Thus, although the government's activities in *Katz* involved no physical intrusion, they were found to have abridged Katz's reasonable expectation of privacy, thus violating the Fourth Amendment.[15]

Even though the Supreme Court has expanded and extended the notion of privacy under the Fourteenth Amendment, not all laws allowing for dissemination of private information have been found to violate the constitutional right to privacy. In *Whalen v. Roe*, the Supreme Court held that a New York law that required the recording of names and addresses of all persons who obtained certain prescription drugs, for which there was both a lawful and unlawful market, with such records sent to a centralized computer file, did not violate any right of privacy protected by the Fourteenth Amendment.[16] On its face, the Court held, the New York program did not interfere with constitutionally protected fundamental rights (such as the right to choose methods of contraception), and requiring such disclosure to representatives of the State did not amount to an impermissible invasion of privacy.[17] The Court also noted that the "remote possibility" of unwarranted disclosures was not a sufficient reason to invalidate the entire patient-identification program.[18]

7 410 US 113 (1973).
8 *Id.* at 155.
9 *Id.* at 155.
10 *Id.* at 163–64.
11 *Id.* at 165.
12 389 U.S. 347 (1967)
13 *Id.* at 351.
14 *Id.* at 543.
15 *Id.*
16 429 U.S. 589, 603–04 (1977).
17 *Id.* at 600, 602.
18 *Id.* at 601–02.

2. Federal Statutory Rights To Privacy

Although many U.S. privacy rights find their roots in the Constitution and common law, many modern statutes also address various types of privacy protection.

The government has the right to collect personal data and use such data for specific purposes, and generally, this right is accompanied by the statutory duty to avoid unwarranted disclosures of such information. For example, the landmark 1974 Privacy Act provides privacy protection by preventing misuse of records by Federal agencies.[19] Government agencies must follow certain procedures in the collection and disclosure of records containing personal information, and the Federal Privacy Act also gives individuals the right to review their records and an opportunity to amend the contents of their records. A companion to the Privacy Act is the Freedom of Information Act, which provides a process by which every person may request access to federal agency records or information, and regulates third party access to government records, including records containing personal information.[20] These two statutes reflect the tension in privacy law – a desire to protect individuals from unwarranted disclosure of information, while at the same time granting access to information.

Some types of information that the government collects could personally identify an individual. Title 13 U.S.C. Section 9 requires that information gathered by the Census Bureau be kept confidential and be used exclusively for statistical purposes.[21] Likewise, the Tax Reform Act of 1976 protects the confidentiality of information disclosed on tax returns, and limits the dissemination of individual tax data to federal agencies other than the Internal Revenue Service.[22]

Individuals are also given the right to engage in communications without the contents of their communication being arbitrarily intercepted and disseminated. The federal wiretap statute, for example, prohibits the interception, recording and disclosure (without court order) of "any wire, oral, or electronic communication" unless one of the parties to the communication, implicitly or explicitly consents.[23] The federal government, in response to modern computer transmission technologies, amended the wiretap statute and enacted the Electronic Communications Privacy Act of 1986 ("ECPA").[24]

Further, the protections of various statutes may overlap. Both the ECPA and a provision of the Stored Communications Act apply to email privacy. The Stored Communications Act requires consent of either the sender or the receiver of email messages before a stored message may be accessed.[25] Other types of communications are also protected by statute. The Mail Privacy Statute makes it illegal for anyone to open mail that is not addressed to them, unless they obtain a search warrant or the addressee's consent.[26]

---

19 5 U.S.C. Section 552a.
20 5 U.S.C. Section 552.
21 Similarly, the Health Research Data Statute, 42 U.S.C. Section 242m, prohibits disclosure of data collected by the National Centers for Health Services Research and for Health Statistics that would identify an individual in any way.
22 26 U.S.C. Section 6103. In view of the importance of protecting personal information obtained by the government, the Computer Security Act of 1987, 40 U.S.C. Section 1441, was enacted to provide for improving the security and privacy of sensitive information in federal computer systems. The Act also requires each federal agency to provide mandatory periodic training in computer security awareness.
23 This statute creates a privacy right for the contents of telephone conversations, telegraph messages, or electronic data sent by wire. *See* 18 U.S.C. Section 2510 et seq. (creating civil and criminal liability for anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication").
24 It is important to note that many of the statutes that purport to give privacy protections contain numerous exceptions, *e.g.*, the ECPA provides exceptions for electronic workplace monitoring. 18 U.S.C. Section 2510 et seq.
25 10 U.S.C. 2702(b)(3).
26 39 U.S.C. Section 3623.

There are numerous statutes that extend privacy rights to consumers and customers. The Financial Privacy Act of 1978, for example, protects certain financial records from disclosure.[27] Under this statute, if a government agency wishes to disclose personal financial information provided to the agency, the individual affected must be provided notice and must authorize disclosure.

The Federal Trade Commission Act ("FTCA") helps makes sure that companies keep the promises they make to consumers about privacy.[28] Under Section 5 of the FTCA, a company that fails to implement necessary security protection of a consumer's personal information may be prosecuted, as such failures may be considered "unfair" or "deceptive" practices. Title V of the Gramm-Leach-Bliley Act ("GLBA") (the Financial Modernization Act of 1999) also sets forth guidelines that restrict the use of consumer information by financial institutions and non-affiliated third parties to whom they transfer such information.

Another example of consumer protection for private information appears in the Fair Credit Reporting Act ("FCRA"), enforced by the Federal Trade Commission, which governs how credit reports may be maintained and used.[29] An extension of the FCRA appears in the Consumer Credit Reporting Reform Act of 1996, which attempts to provide even greater privacy protections to consumers.

Customers of certain services, e.g., telephone, cable, and even video stores are afforded statutory privacy protection. The Privacy of Customer Information Act was enacted as part of the Telecommunications Act of 1996 to regulate the disclosure of names, addresses, and other proprietary information of customers who obtain telephone service.[30] Similarly, the Cable Communications Policy Act of 1984 regulates the disclosure of names and address information of subscribers, as well as their viewing habits.[31] The Act requires an annual disclosure of information practices, including the type of personal data that is collected and the operator's data disclosure policies. The Video Privacy Protection Act operates in a similar manner, regulating the gathering of the name and address information of patrons who rent video materials.[32] The Act prevents disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material."[33]

Individuals also enjoy various statutory privacy rights with regard to their health and medical treatment. One of the most widely known statutes that protect health information is the Health Insurance Portability and Accountability Act ("HIPAA").[34] Privacy regulations issued by the Department of Health and Human Services under HIPAA give patients control over use of their protected health information. Additionally, health plans and health care providers must obtain a patient's consent for use and disclosure of protected information in connection with treatment, payment, and health care operations.

If an individual is treated in a federally regulated substance abuse program, the records of the identity, diagnosis, prognosis, and treatment of the patient are confidential

27 12 U.S.C. Section 3401 et seq.
28 15 U.S.C. Sections 41-58.
29 15 U.S.C. Section 1681 et seq.
30 47 U.S.C. Section 222.
31 47 U.S.C. Section 551.
32 18 U.S.C. Section 2710.
33 DVDs, video games, and other types of recordings are now the most popular forms of rentals at video stores. While it appears on the face of this statute that someone renting these types of recordings will also be afforded the same privacy protection as one renting video cassettes, this extension of the Act has yet to be tested. This potential statutory gap exemplifies another situation in which law does not always keep up with technology developments.
34 Pub. Law No. 104-191 Sections 262, 264; 45 C.F.R. Sections 160-164.

under the Drug and Alcoholism Abuse Confidentiality Act.[35] Such information is also specifically protected from use against the subject in any criminal proceeding. It is important to note that this statute only applies to substance abuse programs affiliated with the federal government – the same protections may not be afforded to private programs.

Veterans are also afforded special privacy protection under the Veterans Administration Health Privacy Act, which requires confidentiality in Veterans Administration records on the identity, diagnosis, prognosis, and treatment of any patient, relating to drug abuse, alcoholism or alcohol abuse, infection with the HIV virus, or sickle cell anemia,[36] with some exceptions.

Education is another arena in which personal information privacy rights have been protected, for students and their parents. The Family Educational Rights and Privacy Act ("FERPA") applies to all schools that receive federal funds, to protect the privacy of student education records.[37] Under FERPA, students over the age of 18 and parents of students under 18 have the right to inspect and review their school records, request corrections to records that they believe to be incorrect or misleading, and prevent the release of such information without permission, except under limited circumstances.

The idea that privacy is the "right to be let alone" is reflected in the Telephone Consumer Protection Act of 1991, which places limitations on unsolicited, automated telephone calls to the home, and protects subscriber privacy rights.[38] Similarly, individuals are protected against abusive debt collection practices under the Fair Debt Collection Practices Act of 1977, which aims to eliminate abusive collection practices by debt collectors and to protect individuals against invasions of their privacy.[39]

Other statutes have been enacted in response to use of the internet and the new ways that information can be collected online. The Children's Online Privacy Protection Act of 1998, COPPA, gives parents control over information collected from their children online, and permits parents to control how such information is used.[40]

Various characteristics of an individual are also afforded statutory protection from privacy invasions. The Equal Credit Opportunity Act, for example, restricts inquiries into a credit applicant's sex, race, color, religion, or marital status.[41] The Equal Employment Opportunity Act restricts collection and use of information that could result in employment discrimination on the basis of race, sex, religion, national origin, and a variety of other characteristics.[42] Similarly, the Fair Housing Act restricts the collection and use of information that could result in housing discrimination on the basis of race, sex, religion, national origin and a variety of other factors.[43]

3. State Sources Of Privacy Rights

The Supreme Court has construed provisions in the Bill of Rights to provide some protection to a variety of elements of individual privacy. Yet, there is no general guarantee

35 21 U.S.C. Section 1175; 42 U.S.C. Section 290dd.
36 38 U.S.C. Section 7332.
37 20 U.S.C. Section 1232g .
38 47 U.S.C. Section 227.
39 15 U.S.C. Section 1692 et seq.
40 15 U.S.C. Sections 6501 et seq., 16 C.F.R. Section 312.
41 29 U.S.C. Section1025.
42 42 U.S.C. Section 2000e.
43 42 U.S.C. Sections 3604-05.

of a right to privacy in the Federal Constitution. Most states have followed a similar path in interpreting their own constitutions. Although a limited federal right to privacy has been incorporated through the Fourteenth Amendment to apply to the states, many states have granted even greater protections for privacy rights than the rights afforded to individuals under federal law.

Among the states, there is no single way to define or implement an individual's right to privacy. Some states expressly recognize a right to privacy in their state constitutions. For example, California's State Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[44] In other states, court decisions have established a constitutional right of privacy.[45]

These are not the only differences in sources of protection for state privacy rights. Most states protect their citizens only against intrusions into privacy by state actors. Yet, there are some exceptions. Some states have criminalized the invasion of privacy; some states have merely codified common law actions for invasion of privacy; and some states have recognized greater protections of privacy than those offered at the federal level, at least in certain circumstances.

The amount of privacy protection varies greatly from state to state. Because of the differences in protections offered between the states and the possibility that one state may offer greater protection than another, it is imperative that companies consult the laws of the state(s) that may affect their business interests.

4. Common Law Privacy Rights

Another source for the right to privacy can be found in tort law, which is also state-specific. Invasion of privacy has generally been classified into four distinct torts: appropriation, unreasonable intrusion upon the plaintiff's seclusion or solitude, public disclosure of private facts, and false light in the public eye.[46]

The tort of appropriation is "an invasion of privacy whereby one person takes the name or likeness of another" for commercial gain.[47] The tort of intrusion upon seclusion involves any "highly offensive invasion of another person's seclusion or private life."[48] This type of intrusion can include peeping into a person's home, wire-tapping telephones, and obtaining bank balance information without permission.

A public disclosure of private facts is "the public revelation of some aspect of a person's private life" without a legitimate public purpose. The disclosure is actionable in tort "if the disclosure would be highly objectionable to a reasonable person."[49] Some

44 CAL. CONST. art. I, Section 1; *see also* MONT. CONST. art. II, Section 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.").
45 For example, Georgia does not specifically mention privacy in its constitution, but the Georgia Supreme Court has "expressly recognized that Georgia citizens have a 'liberty of privacy' guaranteed by the Georgia constitutional provision that declares that no person shall be deprived of liberty except by due process of law." *See Powell v. State*, 270 Ga. 327, 329 (Ga. 1998) (citations omitted).
46 *See* RESTATEMENT (SECOND) OF TORTS at Sections 652A-652I.
47 BLACK'S LAW DICTIONARY 110 (8th ed. 2004). A similar concept is the "right of publicity", reflected in Restatement (Third) Unfair Competition Sections 46-47 (1995). The distinction is that privacy protects against "injury to personal feelings," while the right of publicity protects against unauthorized commercial exploitation of a person's name or face. As a practical matter, celebrities generally sue under the right of publicity, while ordinary citizens sue to protect their privacy rights.
48 BLACK'S LAW DICTIONARY 829 (7th ed. 1999).
49 BLACK'S LAW DICTIONARY 497 (8th ed. 2004).

examples include publication of documents relating to medical treatment or sexual relations or photographs of a person in the confines of his or her own home.

Finally, false light liability, in an invasion of privacy claim, is "a plaintiff's allegation that the defendant attributed to the plaintiff views that he or she does not hold and placed the plaintiff before the public in a highly offensive and untrue manner."[50]

The scope and elements of various privacy-related tort claims are more specifically defined in the state law of jurisdictions that recognize these claims as actionable. Thus, companies should be well-versed in tort law principles that could impose obligations relating to the maintenance of privacy interests.

5. Miscellaneous Sources Of Privacy Rights

Another source for privacy rights arises from the obligations of certain professionals, e.g., protection of the confidentiality of disclosures made to a doctor, an attorney, or a religious official, such as a priest. These rights to confidential communications in certain types of relationships are based on ethics codes. Violations of the confidentiality of communications can put a professional's license at risk and possibly rise to the level of a tort. Other sources of privacy protection include evidence codes, at both the federal and state level. In a legal proceeding, certain privileges can be invoked to prohibit the introduction of confidential communications disclosed in protected relationships. The existence of these privileges varies from state to state.[51]

U.S. DISCOVERY REGIME GENERALLY LIBERAL

The core regulation governing civil discovery in U.S. federal courts is Rule 26 of the Federal Rules of Civil Procedure 26 ("Fed. R. Civ. P. 26"). Fed. R. Civ. P. 26(b)(1) requires parties to disclose in discovery, information "regarding any nonprivileged matter that is relevant to any party's claim or defense."[52] Fed. R. Civ. P. 26(b)(1) further states that, "if the discovery appears reasonably calculated to lead to the discovery of admissible evidence," then the information is considered "relevant" even if the information requested is not directly relevant.[53] Thus, Fed. R. Civ. P. 26(b)(1), "permits the discovery of any matter relevant to the subject matter of the pending action, so long as the sought after information is not privileged, even if inadmissible at trial, if the information sought appears reasonably calculated to lead to the discovery of admissible evidence."[54]

POTENTIAL LIMITS ON DISCOVERY: PLEADING STANDARDS

Potential limits on U.S. discovery emerge from a variety of rules and judicial opinions. For example, the U.S. Supreme Court has held, "to survive a motion to dismiss [and thus gain access to the discovery process], a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face."[55] In *Ashcroft v. Iqbal*, the Court extended that pleading standard to all federal civil actions.[56] If the

50 BLACK'S LAW DICTIONARY 636 (8th ed. 2004).The tort of false light invasion of privacy is similar to a claim for defamation.
51 Other potential claims of privilege can sometimes be invoked to protect the privacy of an individual involved in a legal proceeding, *e.g.*, the marital privilege, joint-defense privilege, journalist's privilege, psychotherapist-patient privilege, accountant-client privilege, and the privilege against self-incrimination.
52 FED. R. CIV. P. 26(b)(1).
53 *Id.*
54 *Putman v. Lima Auto Mall*, No. 08-MC-86-MJR-CJP, 2008 U.S. Dist. LEXIS 98807, at *3 (S.D. Ill. 2008).
55 *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007).
56 *See Ashcroft v. Iqbal*, 129 S.Ct. 1937, 1953 (2009) ("Our decision in *Twombly* expounded the pleading standard for 'all civil actions,' and it applies to antitrust and discrimination suits alike.")

complaint is deficient, these pleading standards, the complainant is not entitled to discovery.[57] Thus, the pleading standard should not allow plaintiffs to engage in pure "fishing expeditions." Thus, the Rules do not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions."[58]

Further, courts may grant a motion to stay discovery if a motion to dismiss is filed, where "discovery may be especially burdensome and costly to the parties."[59] In fact, "[t]he Court premised its holding in [*Twombly*] on the policy against a 'plaintiff with a largely groundless claim be[ing] allowed to take up the time of a number of other people, with the right to do so representing an *in terrorem* increment to the settlement value.'"[60] The Court furthered this policy in its *Twombly* decision by indicating "that a district court was justified in insisting on some specificity in the pleading in [a]…case before proceeding with potentially massive and expensive discovery."[61] Thus, "a defendant should not be burdened with the heavy costs of pretrial discovery that are likely to be incurred in a complex case unless the complaint indicates that the plaintiff's case is a substantial one."[62]

PRIVACY AS A DISCOVERY "BURDEN"

Fed. R. Civ. P. 26(b)(2)(B) provides specific limitations on the discovery of electronically stored information. The rule provides that a party need not "provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." The burden of showing that the requested information is not reasonably accessible falls on the producing party that has to produce the requested information.[63] However, even "[i]f that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause," while specifying conditions for the discovery as it sees fit.[64]

The rules specifically contemplate limitations on discovery related to "burden," which may include privacy concerns.[65] Fed. R. Civ. P. 26(b)(2)(C)(iii) requires courts to limit the frequency or extent of discovery when "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues." Advisory Committee notes to the Rules expressly reference "privacy" as a burden concern.[66] And courts have held that "the word 'burden' applies to the adverse consequences of the disclosure of sensitive, albeit unprivileged, material," including "risks to …privacy."[67] Thus, courts may use a burden

57 *See id.* at 1954 ("Because respondents complaint is deficient under Rule 8, he is not entitled to discovery, cabined or otherwise.")
58 *Id.* at 1950.
59 *See Coss v. Playtex Products*, No. 08-cv-50222, 2009 U.S. Dist. LEXIS 42933, at *3 and 9 (N.D. Ill. 2009) ("The court may grant a motion to stay discovery for a number of reasons, including the filing of a motion to dismiss. Stays are often deemed appropriate where…discovery may be especially burdensome and costly to the parties."…"If the complex case is one susceptible to the burdensome and costly discovery contemplated by [*Twombly*] and *Iqbal*, the district court should limit discovery once a motion to dismiss for failure to state a claim has been filed.")
60 *Id.* at *4-5.
61 *Id.* at *5.
62 *Beck v. Dobrowski*, 559 F.3d 680, 682 (7th Cir. 2009) (Posner, J.). *Coss,* 2009 U.S. Dist. LEXIS 42933, at *8. "Post *Iqbal*, the policy against burdensome discovery in complex cases during the pendency of a motion to dismiss holds fast."
63 *See* FED. R. CIV. P. 26(b)(2)(B) ("On motion to compel discovery for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost.")
64 *Id.* ("If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.")
65 FED. R. CIV. P. 26(b)(2)(C)(iii); FED. R. CIV. P. 26(c)(1).
66 *See* FED. R. CIV. P. 34, Advisory Committee Notes (1970) ("Protection may be afforded to claims of privacy or secrecy," pursuant to FED. R. CIV. P. 26(c)).
67 *Bennett v. Kingsbridge Heights Rehabilitation Care Center*, No. 07-cv-9456 (LAK), 2009 WL 3294301, at *3 (S.D.N.Y. 2009).

analysis to limit discovery when the burden of the infringement on an individual's privacy caused by the discovery outweighs the likely benefits of discovery.[68]

Additionally, Fed. R. Civ. P. 26(c)(1) provides that a court may, for good cause, issue a protective order limiting discovery that would cause annoyance, embarrassment, oppression, or undue burden or expense for a party or person.[69] The U.S. Supreme Court, in *Seattle Times Co. v. Rhinehart*, held that the "good cause" standard of Fed. R. Civ. P. 26(c)(1) is satisfied if the protective order serves to curb abuse stemming from discovery.[70] The Court in *Seattle Times Co. v. Rhinehart* explained how protective orders may be used to protect privacy:

> It is clear from experience that pretrial discovery by depositions and interrogatories has a significant potential for abuse. This abuse is not limited to matters of delay and expense; discovery also may seriously implicate privacy interests of litigants and third parties. The Rules do not distinguish between public and private information. Nor do they apply only to parties to the litigation, as relevant information in the hands of third parties may be subject to discovery. There is an opportunity, therefore, for litigants to obtain — incidentally or purposefully — information that not only is irrelevant but if publicly released could be damaging to reputation and privacy. The government clearly has a substantial interest in preventing this sort of abuse of its processes.[71]

Certain specific federal laws may set forth specific standards for protective orders to protect information covered by a federal privacy law or regulation to be allowed.[72]

Under Fed. R. Civ. P. 26(b) & (c), a court may allow discovery to progress unimpeded, or it can set specific limitations on what must be produced. A court may require the requesting party to pay some or all of the costs of the discovery request in order to reduce the burden on the producing party.[73] Courts may also use a sampling procedure to determine whether requested material is likely to be relevant, before requiring full compliance with a discovery request.[74]

There are also several federal statutes that grant privacy rights specifically affecting discovery in the private sector. One example of these federal statutes is Title V of the Gramm-Leach-Bliley Act ("GLBA"), which provides that "except as otherwise provided in this chapter, a financial institution may not…disclose to a nonaffiliated third

---

68 *See, e.g. Labrew v. City of New York*, No. 07-cv-4641 (DAB)(DFE), 2009 WL 3747165, at *1 (S.D.N.Y. 2009) ("Pursuant to Fed.R.Civ.P. Rule 26(b)(2)(C)(iii), I hereby determine that the privacy burden of the proposed discovery outweighs its likely benefit."). *See also Stampf v. Long Island Railroad Co.*, No. 07-cv-3349 (SMG), 2009 WL 3628109, at *2 (E.D.N.Y. 2009) ("The burden of producing the discovery sought by plaintiff would be substantial…the nature of the material is such that its production would invade the privacy of Mr. Jackson.")

69 *See* FED. R. CIV. P. 26(c)(1) ("The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense…").

70 467 U.S. 20, 34 (1984).

71 *Id.* at 34-35 (1984).

72 Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Implementing regulations, for example, set forth terms for such an order. *See* 45 C.F.R. Section164.512(e)(1)(v) ("a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and (B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.")

73 *See, e.g., OpenTV v. Liberate Technologies*, 219 F.R.D. 474, 479 (N.D. Cal. 2003) (holding that the cost of restoring inaccessible data to accessible data should be equally split between the parties).

74 *See, e.g., Zubulake v. UBS Warburg*, 217 F.R.D. 309, 323-24 (S.D.N.Y. 2003) (requiring the restoration of sample backup tapes to determine the likely relevance of the information before requiring the restoration of all the requested backup tapes).

party any nonpublic personal information."[75] Thus, the GLBA may limit or preclude plaintiffs from obtaining discovery of any nonpublic personal information of individuals from financial institutions.

Other federal statutes that limit discovery by granting privacy rights include: the Family Education and Privacy Rights Act,[76] which regulates the disclosure of educational records; the Health Insurance Portability and Accountability Act of 1996,[77] which protects individually identifiable health information; and the Americans with Disabilities Act,[78] which provides for the confidentiality of certain health information held by employers.

RECENT U.S. CASES BALANCING PRIVACY VERSUS DISCOVERY

The Supreme Court's recent decision in *City of Ontario v. Quon*[79] offers an important perspective on the balance between privacy and discovery. In that case, a municipal police department issued pagers to its officers. The department sought to review text messages sent by an officer over the pager, in an attempt to determine why that pager (and others) had exceeded the monthly volume limit, triggering additional charges. After reviewing transcripts provided by the telephone company, the police department found that many of the plaintiff officer's text messages sent from that pager, during work hours, were sexually explicit. On this basis, the department disciplined the plaintiff.[80] The plaintiff, Officer Quon, challenged the department's actions under the Fourth Amendment and the federal Stored Communications Act.[81]

The Court rejected Quon's argument, noting that while "the [Fourth] Amendment guarantees a person's privacy, dignity, and security against arbitrary and invasive governmental acts, without regard to whether the government actor is investigating crime or performing another function," the protection does not extend to instances where the search is reasonable, as here, because it has a legitimate purpose.[82]

The Stored Communications Act ("SCA"), addressed in part in lower court decisions in *Quon*, generally bars providers of electronic communications services from divulging the contents of communications made over their service.[83] The Act provides several exceptions, including power to divulge communications to law enforcement agencies if the contents appear to pertain to the commission of a crime.[84] Under the SCA, when requiring disclosure of such communication, the government must provide notice within 3 days after the service provider begins making copies of such communications (with certain exceptions), and the government must, depending on which type of service is in question, obtain either a warrant, a court order, or a subpoena.

The SCA enacted in 1986, must be constantly reinterpreted as electronic communication moves, in many cases, away from traditional email and toward social networking services such as Facebook.com and Myspace.com. One recent case demonstrates the complexity of the issue. In *Crispin v. Christian Audigier, Inc.*, the court relied on the SCA to quash subpoenas served on several social networking sites in an

75 15 U.S.C. Section 6802(a).
76 20 U.S.C. Section 1232g.
77 42 U.S.C. Section 1320d.
78 42 U.S.C. Section 12112(d)(4)(C).
79 130 S. Ct. 2619, 177 L. Ed. 2d 216 (2010).
80 *Id.* at 218-19.
81 U.S. CONST. amend. IV; and Stored Communications Act, 28 U.S.C. Sections 2701-2712 (2006).
82 *Quon*, *supra* note 1, at 225.
83 28 U.S.C. Sections 2701-2702 (2006).
84 *Id.* at Section 2702.

artwork infringement case, reasoning that private email-type messages between users fell within the ambit of the SCA.[85] Remanded and left open, though, was the question whether posts to a user's "wall," a personalized online message board, were covered by the SCA; this, the court held, would depend on whether such communications are in fact private.[86] Depending on the individual's account privacy settings, the "wall" may be visible to many different subsets of individuals, or invisible to all.

As the *Quon* case exemplifies, courts in the United States have struggled to fashion a definition of privacy in the work environment. In *Quon*, an employer was found not to have violated an employee's Fourth Amendment rights by reviewing transcripts of text messages, when done for the legitimate purpose of determining the reason for over-use charges from the pager service provider.[87] On the other hand, in at least one recent decision a U.S. court accorded protection to personal communications sent via an employer-owned computer. In *Stengart v. Loving Care Agency, Inc.*, the New Jersey Supreme Court found that an employee's communications with her attorney, via her personal email account but on her employer's computer, were protected.[88] The court relied on attorney-client privilege as the basis for this claim of privacy, rather than the Fourth Amendment. In this instance, the court found a right to privacy even though the employer had an express written policy telling employees that they should expect no privacy for communications sent on company hardware.[89]

The *Stengart* decision may have limited impact in other cases. In several earlier decisions, U.S. courts have sided with the employer in finding that employees were not guaranteed privacy in their communications over employer-owned systems. In *Bourke v. Nissan*, a manager at a car dealership, while demonstrating to employees how to use the company email system, selected at random for the demonstration a message from plaintiff employee Bourke's email inbox, which happened to contain sexually explicit material.[90] After the incident was reported to management, the employer examined Bourke's other emails, and relied in part on the large number of explicit personal emails in giving Bourke a poor performance evaluation, criticizing her for the amount of time she spent on personal matters while at the office. The court sided with the employer, finding that Bourke had no right to privacy in her emails.

In a later case with better facts for the plaintiff, another court again sided with the employer. In *Smyth v. Pillsbury*, an employer fired an employee for sending inappropriate emails over his work email account, even though the employer had previously provided express assurances that employees would not be terminated on the basis of material sent over the email system.[91] The court concluded, "even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy."[92] These cases are more representative of the current norm.

85 2010 U.S. Dist. LEXIS 52832, at *42-43 (C.D. Cal. May 26, 2010).
86 *Id.*
87 *Quon*, *supra* note 1, at 225.
88 973 A.2d 390, 402 (N.J. 2010).
89 *Id.*
90 No. B068705, slip op. (Cal. Ct. App. July 26, 1993).
91 914 F. Supp. 97, 98-99 (E.D. Pa. 1996).
92 *Id.* at 101.

ANALOGY TO PRIVACY CONCERNS IN TRADE SECRET CASES

Like privacy, the issue of trade secrets often presents a challenge in the discovery context. American courts employ several tools with which to protect trade secrets during the discovery process, which they have employed in recent years. In *Hope for Families & Community Services, Inc. v. Warren*, for example, plaintiffs sought production of information in a gambling regulation dispute, which the defendants objected to, arguing that the materials contained trade secrets about the company's competitive practices.[93] The judge chose a middle path by limiting the discovery request but nonetheless ordering production of documents containing trade secrets, relying on a previously-entered protective order to maintain the secrecy of the documents.[94]

The court in *Opperman v. Allstate New Jersey*, used a similar limiting order when an interested third party opposed the plaintiff's request to access the third party's proprietary software, which had been used by the defendant.[95] The court ordered the third party to provide an accessible version of the software to the plaintiff, but entered a discovery confidentiality Order as a means of limiting access to and use of the software.[96]

In other recent instances, U.S. courts have been more deferential to parties seeking to protect trade secrets during the discovery process. In a class action lawsuit stemming from unsolicited advertisements faxed by the defendant to the plaintiffs, the plaintiffs sought production of defendant's database, which contained telephone numbers for each of the individuals solicited.[97] The defendants opposed production of the database, arguing that it contained customer information that was protectable as a trade secret. The court agreed, and denied the plaintiffs' motion to compel.[98]

In another recent case, the court also granted significant deference to the party seeking protection of its trade secrets.[99] The defendant sought production of documents that contained trade secrets. After the parties failed to agree to a proposed protective order, the court sided with the plaintiff, and allowed the plaintiff to mark entire documents as confidential as long as done in good faith.[100]

Similarly, in another recent opinion, the court deferred to the party seeking to protect its trade secrets.[101] In that case, the plaintiffs sought production of an interested third party's hard drives, and the third party opposed the motion and sought a protective order.[102] The court allowed the third party to search its own hard drives, rather than hand them over, and did not require the third party to produce documents containing trade secrets.

93 250 F.R.D. 653, 660-61 (M.D. Ala. 2008).
94 *Id.* at 662.
95 2008 U.S. Dist LEXIS 95738, at *3-6 (D.N.J. Nov. 24, 2008).
96 *Id.* at 12-13.
97 *Hypertouch, Inc. v. Superior Court*, 27 Cal. Rptr. 3d 839, 841 (Cal. Ct. App. 2005).
98 *Id.* Later in the case, the plaintiffs learned that the defendants had destroyed a separate database, which contained a list of all the phone numbers that had contacted the company to request it stop sending faxes. At that point, the judge ordered the defendant to use its database to contact those individuals who had requested that they not receive any further faxes, in order to invite them to join the class.
99 *Containment Technologies Group v. Am. Soc'y of Health Sys. Pharmacists*, 2008 U.S. Dist. LEXIS 80688, at *2 (S.D. Ind. Oct. 10, 2008).
100 *Id.* at 17-18.
101 *Daimler Truck N. Am. LLC v. Younessi*, 2008 U.S. Dist. LEXIS 86022 at *13-14 (W.D. Wash. June 20, 2008).
102 *Id.* at 3.

ANALOGY TO PRIVACY IN PRIOR SEXUAL HISTORY CASES

Rule 412 of the Federal Rules of Evidence ("FRE") governs the admissibility of evidence of a party's previous sexual history.[103] Rule 412(a), which bars the admission of evidence offered to prove either that (1) the alleged victim engaged in other sexual behavior or (2) the alleged victim had any sexual predisposition, applies to both criminal and civil cases. Sections (b) and (c), which provide means to admit evidence of sexual history in certain instances, apply only in criminal cases; therefore, the evidence barred from admission in (a) is never allowed in a civil case.

Rule 412, however, applies only to the admissibility of evidence, not to discoverability. Discoverability in a civil case is governed by Fed. R. Civ. P. 26, which allows discovery of "any nonprivileged matter that is relevant to any party's claim or defense."[104] The broad standard for discovery creates a conflict, because a defendant in a sexual harassment suit may seek information during discovery about the plaintiff's sexual history, which is relevant to potential defenses under Fed. R. Civ. P. 26, but not necessarily admissible under Fed. R. Evid. 412. The Advisory Committee Notes to Fed. R. Evid. 412 provide some guidance, stating that "in order not to undermine the rationale of Rule 412, however, courts should enter appropriate orders pursuant to Fed. R. Civ. P. 26(c) to protect the victim against unwarranted inquiries and to ensure confidentiality."

Several cases have set out particular instances in which information about an alleged victim's prior sexual history may be admissible (and discoverable). In *Meritor Savings Bank v. Vinson*, the plaintiff alleged that her supervisor sexually harassed her.[105] The defendant alleged that the plaintiff welcomed the harassment by wearing provocative clothing and discussing sexual fantasies with the defendant. The court found that such evidence is "obviously relevant," and is not "per-se inadmissible."[106]

In certain instances, a party may inadvertently waive the right to prevent discovery of prior sexual acts. For example, a plaintiff seeking damages for emotional distress stemming from an alleged sexual act by the defendant may be required to disclose instances of previous sexual activity, since that would be relevant in determining whether the plaintiff was in fact harmed by the alleged conduct.[107] Likewise, a plaintiff suing for defamation based on statements about his sexual history may open himself up to discovery of his previous sexual history, because such information would help the defendant argue "truth" as a defense.[108]

TOOLS AVAILABLE TO U.S. COURTS TO BALANCE PRIVACY AND DISCOVERY

Fed. R. Civ. P. 26(b) grants federal courts the authority to limit the scope of discovery. A court may grant a party's request to avoid discovery of electronically stored information when the information is not reasonably accessible, per Rule 26(b)(2)(B), or may "specify conditions" (including a shifting of costs) for the discovery. Under Rule 26(b)(2)(C), a court "must limit" the "frequency or extent of discovery" if it makes any of the following determinations: (1) first, that the discovery is unreasonably cumulative or duplicative, or could be obtained from another source more easily; (2) that the party

103 FED. R. EVID. 412.
104 FED. R. CIV. P. 26(b)(1).
105 477 U.S. 57, 60 (1986).
106 *Id.* at 69.
107 *EEOC v. Dank Indus., Inc.* 990 F. Supp. 1138, 1141 (E.D. Mo. 1997).
108 *Condit v. Dunne*, 225 F.R.D. 100, 106 (S.D.N.Y. 2004).

seeking discovery has already had ample opportunity to obtain the information in question through discovery; or (3) that the burden or expense of the proposed discovery outweighs the likely benefit or the amount in controversy.

Courts rely heavily on Rule 26 to limit the scope of discovery. In *Bayer AG v. Betachem, Inc.*, the Third Circuit refused to grant discovery of redacted documents after the opposing party's counsel had the opportunity to review the redacted versions, and had been provided with copies of the unredacted versions.[109] Relying on Fed. R. Civ. P. 26, the court found that the additional discovery, after the opposing party had already agreed to turn over several of the redacted documents, was duplicative. In a similar case, a plaintiff sought the defendant's sales records from 1984-2003, for a case regarding an agreement in force between 1984 and 1997.[110] The court agreed with the defendant, and limited the scope of the discovery request to the applicable years.[111]

As electronic discovery has become commonplace, and increased in cost, Rule 26(b)(2)(B) has taken on greater import. In *Young v. Pleasant Valley School District*, for example, plaintiff parents sued their children's school district after the school retaliated against their children for complaining to the school about a teacher's inappropriate actions.[112] To help prove their case, the plaintiffs sought backup email tapes. The court denied the request under Rule 26(b)((2)(B), based on the fact that the amount at issue in the case was low relative to the cost of searching the backup tapes. The court reached this conclusion even though "the court ha[d] previously found that complaints about [the defendant] contained on the back-up tapes would be relevant or likely to produce relevant material."[113]

Rule 26(c) governs the use of protective orders to ban the discovery of certain types of information. A court may issue a protective order "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense."[114] The protective order can take any of several forms, ranging from, at one extreme, a complete ban to specific, limited conditions on discovery.

In recent federal cases in which the grant of a protective order was at issue, one essential theme emerges. Courts generally require that the movant seeking a protective order demonstrate some specific need for the order. In one case where the plaintiff sought discovery, the defendant failed to provide the requested documents and then sought a protective order, arguing that the request was unduly burdensome.[115] The judge rejected the motion, finding that the request was not specific and did not adequately explain the need for a protective order. In a similar case, a defendant resisting discovery moved for a protective order, arguing that the discovery requested was duplicative, overly burdensome, and likely to reveal trade secrets.[116] The court rejected the defendant's motion for a protective order, noting that "bald generalizations" did not justify a protective order.

109 173 F.3d 188, 192 (3d Cir. 1999).
110 *In re Microcrystalline Cellulose Antitrust Litigation*, 221 F.R.D. 428, 429 (E.D. Pa. 2004).
111 *Id.* at 430.
112 2008 U.S. Dist. LEXIS 10829, at *1-2 (M.D. Pa. Feb. 13, 2008).
113 *Id.* at *3.
114 FED. R. CIV. P. 26(c).
115 *U & I Corp. v. Advanced Med. Design, Inc.*, 2007 WL 4181900 (M.D. Fla. Nov. 26, 2007).
116 *Cartel Asset Mgmt. v. Ocwen Fin. Corp.*, 2010 WL 502721 (D. Colo. Feb. 8, 2010).