

Note on Data Privacy

The Video Privacy Protection Act

The Video Privacy Protection Act of 1988 is also known as the "Bork Bill." Congress enacted the VPPA after a Washington, D.C., periodical published a list of then-Judge Robert Bork's video rentals during his failed nomination to the United States Supreme Court. The VPPA provides as follows:

§ 2710. Wrongful disclosure of video tape rental or sale records

(a) Definitions. For purposes of this section--

(1) the term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term "ordinary course of business" means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) Video tape rental and sale records.

(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer--

(A) to the consumer;

(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if--

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if--

(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) Civil action.

(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award--

(A) actual damages but not less than liquidated damages in an amount of \$ 2,500;

(B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) Personally identifiable information. Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

(e) Destruction of old records. A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

(f) Preemption. The provisions of this section preempt only the provisions of State or local law

that require disclosure prohibited by this section.

Is the Bork Bill constitutional? Consider the following:

Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You, 52 Stan. L. Rev. 1049 (2000):

The difficulty is that the right to information privacy - my right to control your communication of personally identifiable information about me - is a right to have the government stop you from speaking about me. We already have a code of "fair information practices," and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits, whether the communication is "fair" or not. While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.

....

[O]ne sort of limited information privacy law - contract law applied to promises not to reveal information - is eminently defensible under existing free speech doctrine. The Supreme Court explicitly held in *Cohen v. Cowles Media* [501 U.S. 663 (1991)] that contracts not to speak are enforceable with no First Amendment problems. Enforcing people's own bargains, the Court concluded (I think correctly), doesn't violate those people's rights, even if they change their minds after the bargain is struck. Some have criticized this conclusion on the grounds that it slights the interests of the prospective listeners, and this criticism has some force. Still, I think that ultimately the free speech right must turn on the rights of the speakers, and that it's proper to let speakers contract away their rights - and certainly this is the view that the *Cohen v. Cowles Media* Court took. Insisting that people honor their bargains is a constitutionally permissible "code of fair practices," whether information practices or otherwise.

And such protection ought not be limited to express contracts, but should also cover implied contracts (though, as will be discussed below, there are [*1058] limits to this theory). In many contexts, people reasonably expect - because of custom, course of dealing with the other party, or all the other factors that are relevant to finding an implied contract - that part of what their contracting partner is promising is confidentiality. This explains much of why it's proper for the government to impose confidentiality requirements on lawyers, doctors, psychotherapists, and others: When these professionals say "I'll be your advisor," they are implicitly promising that they'll be confidential advisors, at least so long as they do not explicitly disclaim any such implicit promise.

Laws that explicitly infer such contracts from transactions in which there's no social convention

of confidentiality are somewhat more troublesome, especially if they require relatively formal disclaimers. Imagine, for instance, a law providing that all questions by reporters will be interpreted as implicitly promising not to quote the source by name in a published article, unless the source consents in writing after being given full disclosure of the true purpose for which the quote is to be used. Or consider a law providing that people who buy a product implicitly promise to give the seller equal space to respond to any negative article they publish about the product, unless the seller consents in writing after being given full disclosure of the true purpose for which the product is being bought. Though journalists could avoid the restriction by getting the requisite explicit consent, the request for the consent may deter many of the sources and especially many of the sellers; and this in turn may deter journalists from publishing hostile reviews or stories that include quotes which show the sources in a bad light.

These concerns may justify treating the *Cohen v. Cowles Media* principle as applicable only to those implied contracts where confidentiality really is part of most people's everyday expectations. This would mean the implicit contract theory could uphold laws that by default prevent lawyers, doctors, psychiatrists, sellers of medical supplies, and possibly sellers of videos and books from communicating information about their customers; but it wouldn't uphold laws that by default prevent reporters (who are notorious for communicating embarrassing things, not keeping them confidential) from revealing what was said to them, prevent consumers from reviewing products, or prevent sellers of groceries or shoes from communicating who bought what from them. I doubt that most of us expect that someone selling us our food is implicitly promising to keep quiet about what they sold us.

On the other hand, I'm not sure that such a narrow application of *Cohen v. Cowles Media* is proper or ultimately workable. It's often hard to determine exactly what most people expect. When someone buys a video, especially a video whose title he wouldn't want associated with his name, he probably assumes that the video store won't publicize the purchase, at least in part because a video store that does publicize such purchases would lose a lot of business. But is he assuming that the video store is promising not to publicize such a purchase? He probably isn't even thinking about this.

If he is assuming such a promise, is he assuming that the video store is promising not to communicate information about such a purchase at all, or only promising not to pass it along to the public or his neighbors, while reserving the right to communicate it to others in the same business? Again, most buyers probably have not even thought about the matter. One advantage of statutory default rules is precisely that they clarify people's obligations instead of leaving courts to guess what people likely assumed.

So I tentatively think that a legislature may indeed enact a law stating that certain legislatively identified transactions should be interpreted as implicitly containing a promise of confidentiality, unless such a promise is explicitly and prominently disclaimed by the offeror, and the contract together with the disclaimer is accepted by the offeree. True, this might justify laws that treat reporters as implicitly promising that they won't reveal or even quote their sources, which troubles me. But so long as the implicit promise is genuinely disclaimable, I'm not too troubled.

Even if this might eventually lead to the reporter hypothetical, I don't think too much would be lost; and what is gained from allowing statutorily defined default nondisclosure rules is the clear enforceability of promises that often are reasonably inferred by one of the contracting parties, and that can be important parts of the bargain.

Furthermore, though *Cohen v. Cowles Media* involved traditional enforcement of a promise through a civil suit, there should be no constitutional problem with the government enforcing such promises through administrative actions, or using special laws imposing presumed or even punitive damages for breaches of such promises. I suspect that even with purely contractual remedies, the threat of class action suits could be a powerful deterrent to breaches of information privacy contracts by e-commerce sites, especially since the suits would create a scandal: In the highly competitive Internet world, a company could lose millions in business if people hear that it's breaking its confidentiality promises. But I think it would be constitutional for the government to try to increase contractual compliance either by providing an extra incentive for aggrieved parties to sue or by bringing a complaint itself. Though breach of contract has traditionally been seen as a purely private wrong, to be remedied through a private lawsuit, it's similar enough - especially when it's willful - to fraud or false advertising that there's nothing startling about a government agency such as the Federal Trade Commission prosecuting some such breaches itself.

The great free speech advantage of the contract model is that it does not endorse any right to "stop people from speaking about me." Rather, it endorses a right to "stop people from violating their promises to me." One such promise may be a promise not to say things, and perhaps there may even be special defaults related to such promises or special remedies for breaches of such promises. But in any event, the government is simply enforcing obligations that the would-be speaker has himself assumed. And such enforcement, in my view, poses little risk of setting a broad precedent for many further restrictions, precisely because it is founded only on the consent of the would-be speaker, and thus cannot justify the many other restraints - such as the Communications Decency Act, database protection legislation, and so on - to which the speaker has not consented.

B. Limitations

Contract law protection, though, is distinctly limited, in two ways.

First, it only lets people restrict speech by parties with whom they have a speech-restricting contract, express or implied. If I make a deal with a newspaper reporter under which he promises not to identify me as a source, I can enforce the deal against the reporter and the reporter's employer, whom the reporter can bind as an agent. But if a reporter at another news outlet learns this information, then that outlet can publish it without fear of a breach of contract lawsuit. Likewise, there are no First Amendment problems with an employer suing an employee for breach of an express or implied nondisclosure agreement, but if the employee leaks the information to a newspaper, the employer can't sue that newspaper, at least under the *Cohen v. Cowles Media* theory. The newspaper simply hasn't agreed to anything that would waive its First

Amendment rights, which is the premise on which *Cohen v. Cowles Media* rests. The disclosure tort would similarly not be justifiable under a contract theory.

Second, *Cohen v. Cowles Media* cannot validate speech-restrictive terms that the government compels a party to include in a contract; the case at most validates government-specified defaults that apply unless the offeror makes clear that these terms aren't part of the offered deal. Thus, while the government may say "Cyberspace sales contracts shall carry an implied warranty that the seller promises not to reveal the buyer's personal information," it may not add "and this implicit warranty may not be waived, even by a prominent statement that is explicitly agreed to by a customer clicking on an "I understand, and agree to the contract in spite of this' button."

This flows directly from the rationale on which *Cohen v. Cowles Media* rests: "The parties themselves ... determine the scope of their legal obligations, and any restrictions which may be placed on the publication of truthful information are self-imposed." A merchant's express promise of confidentiality is "self-imposed"; so, one can say, is an implicit promise, when the merchant had the opportunity to say "by the way, I am not waiving my rights to speak about this transaction and am thus not promising confidentiality" but didn't do so. But when someone is legally barred from communicating, even if he explicitly told his contracting partner that he was making no such promise, then such an obligation is hardly "self-imposed" or determined by mutual agreement.

Thus, I certainly do not claim that a contractual approach to information privacy, even with a large dollop of implied contract, is a panacea for information privacy advocates. As Paul Schwartz and others have pointed out, there is much that information privacy advocates may want but that contract will not provide. I claim only that contractual solutions are a constitutional alternative and may be the only constitutional alternative, not that they are always a particularly satisfactory alternative.

C. Government Contracts

Cohen v. Cowles Media does not decide to what extent the government, acting as contractor, may require people to sign speech-restrictive contracts as a condition of getting data from the government itself. This question raises thorny issues of unconstitutional conditions and often of the government's right to restrict access to government records that have historically been in the public domain (such as court records). Unfortunately, the Supreme Court case that some thought would help resolve this matter was decided on procedural grounds, and the dicta in the many opinions in that case shed little light on exactly where the Court would have come down had it confronted the question on the merits. I deal with this issue by setting it aside. [*1063]

D. Contracts with Children

Finally, this discussion of contracts presupposes that both parties are legally capable of entering into the contract and of accepting a disclaimer of any implied warranty of confidentiality. If a cyber-consumer is a child, then such an acceptance might not be valid. This is also a difficult

issue, but one that is outside the scope of this Article.

Paul M. Schwartz, Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence, 52 Stan. L. Rev. 1559 (2000)

In my judgment, . . . the Bork Bill and similar privacy statutes do not represent an unconstitutional silencing of parties under the First Amendment. Rather, so long as they are viewpoint neutral, these laws are a necessary element of safeguarding free communication in our democratic society. . . .

[F]air information practices can best be thought of as fulfilling two normative roles regarding communicative discourse. First, these rules help maintain the boundary between public [*1564] discourse and the other realms of communication. This role is largely fulfilled by the nondisclosure subset of fair information practices. For example, the Bork Bill's prohibition on the release of video rental information keeps these data from becoming part of public discourse. . . .

Second, standards of fair information practices serve to safeguard deliberative democracy by shaping the terms of individual participation in social and political life. [A] democratic order depends on both an underlying personal capacity for self-governance and the participation of individuals in community and democratic self-rule. Privacy law thus has an important role in protecting individual self-determination and democratic deliberation. By providing access to one's personal data, information about how it will be processed, and other fair information practices, the law seeks to structure the terms on which individuals confront the information demands of the community, private bureaucratic entities, and the State. Attention to these issues by the legal order is essential to the health of a democracy, which ultimately depends on individual communicative competence. . . .

. . . .

Today, as a result of evolving models for health care providers and insurers and accompanying alterations in the use of personal health care information, the idea of looking for explicit or implicit understandings of confidentiality based on "most people's everyday expectations" is to rely, at best, on guesswork. In the age of managed care, health maintenance organizations, and physician practice groups, a patient's most important relationships are less with a single medical professional than with a variety of institutions. The use of personal data by these organizations, which know the patient largely through her health care records, are not easily structured by searching for anyone's implicit or explicit understandings of privacy. Indeed, these understandings themselves are largely shaped by how data are used. The actual circumstances of personal data use have tremendous normative power to mold our expectations of informational privacy.

[M]odern health care law is increasingly public law. . . . American law increasingly refuses to allow the terms for the use of personal medical data to be shaped primarily by private parties through fully customized negotiations. The Department of Health and Human Service's (HHS) draft guidelines for personal health care information are only the most recent and elaborate of such attempts to limit private parties' contractual ability to negotiate privacy standards. Freedom of contract is severely limited in the context of medical records, and Volokh's proposal to re-enshrine it seems quaint and anachronistic. Depending on one's reading of the past, it may also be ahistoric. Health care confidentiality itself arguably arises in American law less from any exclusive basis in contract than from the introduction of fiduciary concepts to restrict contract. . .

Any effective scheme of privacy controls must be tied to and follow data through their different applications because the same personal information is increasingly shared in a multiplicity of settings. Due to multi-dimensional use of health care data, two-party private contractual negotiations cannot be relied upon to develop the necessary standards for personal health care data. . . . Purely private multi-party negotiations are problematic because of the public interest in how health care information is used, as well as the lack of patient privacy with some of the most important data processing entities, who receive health care data far downstream from patients. One significant consequence of this phenomenon of dispersed data use occurs in cyberspace, where a recent empirical survey has found that few health Web sites maintain a chain of trust with third parties on their site. According to this study, even Web sites with privacy policies regarding their own use of personal data may not oversee or otherwise limit the data processing of their affiliates. The example of medical data suggests that the State has ample reasons not to allow the bounds of communicative discourse regarding personal data to be hammered out by private parties alone.

. . . .

Consider the guarantee in the HHS draft guidelines of an individual's ability to inspect and copy one's medical records, a right which only twenty-eight states provide at present. This example points to the role of fair information practices in maintaining personal integrity against the onslaught of bureaucratic organizations. . . . [I]ndividuals who are expected to negotiate the terms of information privacy will be hard pressed to do so if they are not even permitted to examine their own records.

Moreover, . . . the State currently has an essential role in creating conditions for a functioning privacy market and in stimulating privacy norms that prevent groups, norm entrepreneurs, and the government itself from being excessively meddlesome. . . . [S]uch market-correcting and norm-shaping activities can serve an important constitutive function for democratic society.

. . . .

Volokh creates a constitutional obligation that all privacy statutes be, in the language of contract law, non-mandatory. . . . The legislature may set a default, but only so long as it is disclaimable.

[This] shifts power to large commercial entities with market power and away from those individuals whose personal data are collected and processed. The resulting agreements, even when explicit in their privacy terms, may, nevertheless, be contracts of adhesion. . . .

[Moreover,] American law places significant limits on the ability of private parties to fully shape the terms for the use of personal medical data. It restricts fully customized negotiations because of the overriding public interest in certain kinds of access and restrictions on personal data use. In health care as well as certain other societal sectors, allowing exclusive bilateral power to private parties to determine the scope of information contracts would have a negative impact on society as a whole. For example, public health in the United States would be worse off if physicians and patients were left to customize their own rules for access to medical data for health care research. Under these circumstances, significant data might become inaccessible to health care researchers. Equally problematic would be fully customized rules between physicians and patients that restricted access to treatment information for fraud or malpractice purposes. Due to the central role in financing health care by such third parties as government, insurers, and employers, an exclusive interest in customizing information rules cannot rest with physicians and patients alone.

Neil M. Richards, Reconciling Data Privacy and the First Amendment, 52 UCLA L. Rev. 1149 (2005)

. . . . The Database Problem

. . . Governments have been keeping records about their citizens for centuries, most notably tax and criminal records. In the nineteenth century, the federal census raised what we would today call privacy concerns and federal law was amended to protect the confidentiality of information collected by the government. In the twentieth century, with the expansion of American government during and after the New Deal period, dozens of national government agencies including the FBI, the Internal Revenue Service, the military, and the Social Security Administration began keeping trillions of records on individual citizens. The invention and spread of increasingly cheaper and more capable computers only facilitated this process, particularly as the use of social security numbers as uniquely effective personal identifiers enabled agencies to link records and integrate them with other databases, including state and private databases. As the Supreme Court has recognized, modern government possesses an "accumulation of vast amounts of personal information in computerized data banks or other massive government files," including information taken from "the collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of our criminal laws."

Public sector databases do create significant privacy problems, including increasing the risk of identity theft, chilling expressive but eccentric behaviors, revealing embarrassing information to private parties, and raising the specter of an Orwellian state. But such problems can be addressed

(at least at a theoretical level) through ordinary public law rules without any significant constitutional impediments. No one suggests that the government has a right to publish any and all secrets it learns about its citizens absent a need to do so; indeed, the Supreme Court has stated on several occasions that individuals have a constitutional right to prevent the government from making public at least certain kinds of information about themselves.

The same technological advances that have permitted the creation of public sector databases have also allowed businesses and other private-sector entities to keep ever larger and more detailed records about individuals. These records can be created from a variety of sources, including publicly available government records, human resource databases, promotional activities such as contests and mass mailings, and transactional data from noncash purchases, frequent shopper programs, and Internet and telephone use. Information collected from these sources often has more value as a saleable commodity than for the purposes for which it was originally collected. Indeed, corporations are eager to acquire many different kinds of information about consumers, including information about their lifestyles, tastes, and even psychological profiles. Such information is provided by the "profiling industry," a group of companies that aggregate information contained in private databases to create consumer profiles that are then offered for sale to interested parties, be they private or public. The level of detail contained in such profiles is striking, and can include information such as a person's social security number, shopping preferences, health information (including diseases and disorders suffered), financial information, race, weight, clothing size, arrest record, lifestyle preferences, hobbies, religion, reading preferences, homeownership, charitable contributions, mail order purchases and type, and pet ownership. Such information can be bought for as little as \$ 65 per thousand names, categorized by the type of consumer sought by marketers. One profiling company was reported to have personal and private information about virtually every consumer in the United States, Britain, and Australia. In addition to being intrusive and deeply unsettling to many people, the multibillion dollar profiling industry provides the lifeblood of data on which the direct marketing industry survives.

At the practical level, such activities raise at least four kinds of privacy concerns. First, databases can be used to process "sensitive information" - nonnewsworthy but nonetheless potentially embarrassing or highly personal information. Most people would be horrified if this information floated freely from database to database. Second, "uber-databases" can be created, composed of nonsensitive information in such enormous quantities that the database constitutes a highly detailed dossier of a person's entire existence. Third, the information contained in consumer profiles can be quite inaccurate. Finally, there are no meaningful legal requirements that personal information in consumer profiles be kept securely. If used improperly, the sheer level of detail contained in consumer profiles can facilitate crimes such as identity theft, stalking, or harassment.

Large-scale private databases also significantly raise the stakes for government surveillance. Governments have long used private records to spy upon their citizens - often with sinister consequences - and the availability of larger and more detailed private records about people makes such forms of surveillance easier for governments to engage in. Indeed, recent activities

by the federal government to investigate and forestall terrorism have frequently relied on computerized private-sector customer records containing financial, airline passenger, and other data. The government also has been contracting increasingly with private businesses, by acquiring databases of personal information and funding novel private-sector data collection projects. To the extent such private data collection is not state action, it allows the government, in effect, to outsource surveillance beyond the scope of otherwise applicable statutory and constitutional restrictions.

.....

Information collection by nonmedia entities raises even fewer First Amendment concerns than does newsgathering by the press. And if there are essentially no First Amendment problems with subjecting the press to the basic principles of generally applicable laws, privacy rules regulating data collection by nonmedia entities fall outside the scope of the First Amendment as well. Thus, because reporters cannot claim a First Amendment privilege to gather information in disregard of tort and property law, it is difficult to envision businesses mounting a colorable free press challenge to consumer-protective privacy rules regulating commercial data transactions. This is particularly true for rules that regulate the commercial relationship between consumers and businesses. In sum, because there are no First Amendment problems with using generally applicable property and tort law to separate the private sphere from the public sphere, the First Amendment critique is simply inapplicable to information collection rules.

.....

The second category of information flow regulations are restrictions on information use placed on recipients of data. Information use is an analytically distinct activity from information collection, but it is similarly unproblematic from a First Amendment perspective. Information use rules regulate the ways in which data about individuals can be processed, applied, or otherwise used by a person or organization. This category of rules does not include the transfer, sale, or disclosure of the data to third parties. Information use rules that are relevant to the data privacy debate include the so-called "secondary use prohibition": the requirement that data collected for one purpose may be used for that purpose only, absent consent. For example, the secondary use prohibition might operate to bar an Internet Service Provider from using the fact that a person visits political fringe or sex-oriented web sites from using that information to send them personalized advertisements. Alternatively, a use rule might prevent a private business that collects my personal information as part of a transaction from including that information in a customer marketing database. Other sorts of information use rules include a prohibition on the use of social security numbers to organize, combine, assemble, and process consumer data profiles more easily.

As with information collection rules, information use rules permeate the common law and statute books of all jurisdictions. For example, professional ethics rules prohibit lawyers from using client information for any purpose unrelated to the client's interests. It is also a violation of

numerous federal and state antidiscrimination laws to use the fact that a person is a member of a protected class to deny them equal treatment, or to take any one of a variety of other actions. Similarly, the federal Fair Credit Reporting Act places a wide variety of restrictions on the use of consumer data contained in credit reports, including limiting uses to an enumerated list, including credit review, insurance underwriting, and employment purposes. Employers using credit reports for employment purposes are also prohibited by the Act from any use inconsistent with applicable equal opportunity employment rules. Trade secret law prohibits the use or disclosure of another's trade secrets. Similarly, federal patent law prohibits the use of information contained in someone else's patent to build the invention described in that patent. States place use conditions on social security numbers and information obtained from their motor vehicle records, while federal law places similar use restrictions on census data.

The Electronic Communications Privacy Act also imposes a use restriction on information that is obtained in violation of its information collection prohibition on intercepting the contents of electronic, wire, or aural communications. ECPA's information use prohibition has been upheld in a variety of contexts involving different uses of information, including the use of intercepted communications from a commercial rival, *inter alia*, to create a competing product, to read a document or listen to a recording obtained as a result of illegal interception, to invest in securities, to take adverse employment actions against employees or subordinates, to use in family or criminal court proceedings, to use in criminal or administrative investigations, and possibly to use as the basis for blackmail.

Information use rules, just like information collection rules, are generally held to be outside the scope of the First Amendment under current doctrine. In *Bartnicki v. Vopper*, the Supreme Court assessed the First Amendment implications of the Wiretap Act's prohibition of the use or disclosure of intercepted communications. The Court drew a sharp distinction between the use of a communication under 2511(1)(c) of the Act and its disclosure under 2511(1)(d), reasoning that while disclosures of information could certainly constitute speech, "the prohibition against the 'use' of the contents of an illegal interception in 2511(1)(d) ... [is] a regulation of conduct." As a content-neutral regulation of conduct, ECPA's information use rule would fall outside the scope of the First Amendment unless, like the information collection rules discussed above, it had a substantial effect upon expressive activity. As the Court strongly implied in *Bartnicki*, virtually all of the activities that prior cases have held to constitute a "use" of intercepted information therefore would be constitutionally unproblematic. . . . [I]t is important to note the Court's clear distinction between regulating the use of information - nonspeech conduct largely outside the scope of the First Amendment - and regulating the disclosure of information that in some circumstances (like the radio broadcast at issue in *Bartnicki*) may regulate speech.

The issue of whether an information use rule violated the First Amendment was assessed peripherally in *U.S. West, Inc. v. FCC*, [182 F.3d 1224 (10th Cir. 1999)] in which the telephone companies sought to use customer information they had received for one purpose (providing phone service) for an unrelated purpose (marketing). Laurence Tribe argued on the telephone companies' behalf that their processing of personal data was speech entitled to full First Amendment protection. The Tenth Circuit accepted this version of the First Amendment critique

and partially agreed. Perhaps unwilling to deal with Tribe's somewhat befuddled argument that the use and processing of data within a company was speech entitled to greater protection than commercial speech, the court concluded that the regulations as a whole placed a restriction on U.S. West's "targeted speech to its customers ... for the purpose of soliciting those customers to purchase more or different telecommunications services." U.S. West's commercial speech rights were therefore unduly burdened. The use of the information, the court asserted, was "integral to and inseparable from" the commercial solicitation. Applying the Central Hudson test for commercial speech restrictions, the court thus invalidated the regulation by determining that the opt-in requirement did not directly and materially advance the state interest in protecting consumer privacy, and that the regulation was not narrowly tailored because it failed to consider an available, less-restrictive alternative. The court also questioned, without deciding, whether a vague interest in protecting consumers from the embarrassment of the disclosure of their data amounted to a substantial government interest.

The Tenth Circuit's reasoning appears wrong under existing law. The FCC rules allowed the telephone companies to advertise to all of their customers, prohibiting them only from using the information to target the advertisements without approval. The rules were thus an ordinary example of a secondary use prohibition that is common to codes of fair information practices, none of which have been held to violate the First Amendment. The only relevant burden placed on the telephone companies was on their ability to use, absent advance customer approval, the information they collected from those customers in the course of their commercial relationship to "target" advertisements to them - that is, to select those most likely to be receptive to such advertisements. The rules were thus not a regulation of speech at all, but rather a regulation of information use - the business activity of deciding to whom to market products. The only burden placed upon the telephone companies was that their advertisements had to be sent to all of their customers, thus making those advertisements less cost-effective. Conduct (and economic conduct at that) was thus all that was regulated, and the Supreme Court has made clear that conduct can be regulated without implicating the First Amendment. The U.S. West example is thus but another instance of the First Amendment critique persuading courts to ask the wrong questions about the First Amendment - that is, to skip the scope question and ignore whether the activity being regulated is really speech within the scope of the First Amendment.

In sum, under established precedent, the conduct of using information, like the conduct of gathering information, can be regulated through generally applicable laws without implicating the First Amendment in most cases, because information use rules generally regulate nonexpressive conduct rather than speech.

....

The third category of information restrictions implicated by fair information practices are restrictions on the disclosure of personal information. Information disclosure rules regulate the ability of persons in possession of information to communicate, sell, or otherwise transfer that information to others. Information disclosure rules can take a variety of forms, including evidentiary privileges, Warren and Brandeis's tort of disclosure of private facts, video rental

privacy protection, and duties of confidentiality and nondisclosure placed upon lawyers and financial advisers.

American law is replete with legal obligations placed on one person not to disclose information about another. While parties are of course generally free to create contracts that regulate their ability to disclose information, public and private law regimes impose numerous mandatory duties of confidentiality that go beyond the contract of the transacting parties to prevent the disclosure of information through speech or other means. For example, doctors, lawyers, and other professionals owe their clients duties of confidentiality, and can be punished through administrative and tort law remedies if they breach these duties by telling confidences to third parties. These duties of nondisclosure are buttressed by analogous evidentiary privileges, which give clients the ability to prevent their lawyers and doctors from speaking against their interests, presumably even when the content of the testimony would be quite newsworthy. Evidence law goes further and grants testimonial privileges to present and former spouses, psychotherapists, and others.

In the commercial context as well, many legal rules impose duties of nondisclosure or confidentiality. For example, agency law imposes a general duty of confidentiality upon agents not to disclose their principal's information. State trade secret law enforces a mandatory regime of nondisclosure that prohibits, *inter alia*, the disclosure of trade secrets to competitors. Furthermore, some states place nondisclosure rules on social security numbers.

Federal statutory law imposes numerous duties of confidentiality under the federal commerce power. The federal Economic Espionage Act also prohibits the disclosure, sale, or receipt of trade secrets, and punishes individual violations with up to fifteen years imprisonment and institutional violations with fines of up to \$ 10 million. Federal securities, antitrust, and labor law impose numerous duties of nondisclosure of truthful information upon corporations. Recent federal statutes place nondisclosure obligations upon banks with respect to customer information, and upon hospitals with respect to patient medical information. Federal law also imposes duties of confidentiality upon cable companies and video stores, charging them with keeping confidential the videos watched by their customers. ECPA provides that the disclosure of an intercepted communication is a separate violation from the interception and use of that communication. Another provision of federal wiretapping law places a duty of confidentiality upon Internet Service Providers with respect to the content of e-mails sent and received by their customers.

Most commercial nondisclosure or confidentiality rules have never been thought to fall within the scope of the First Amendment's protection. Like other commercial regulations, these rules are properly assessed under rational basis review. However, a few information disclosure rules undeniably restrict speech within the scope of the First Amendment in some circumstances - for example when the tort of publication of private facts is applied to a newspaper that wishes to publish information of public concern that it obtained lawfully. Indeed, much of the historical conflict between the privacy tort and the First Amendment has come as a result of litigation over the ability of the media to publish private facts it had received about subjects it felt to be

newsworthy. The Supreme Court has consistently upheld the right of the established media to publish even the most intimate private facts regardless of any countervailing privacy interest. For example, in *Florida Star v. B.J.F.*, the Supreme Court held that the First Amendment protected a newspaper that had published the name of a rape victim from liability under a privacy tort action, even though a government employee had violated agency policy by disclosing the name to the reporter. Unsurprisingly, the First Amendment critics rely heavily upon this line of cases to argue that "while privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law." Accordingly, First Amendment critics assert that only market-based solutions to the database problem - that is, contract, self-regulation, or privacy-enhancing technological solutions - are cognizable options given the dictates of the First Amendment.

.....

[W]hile privacy and speech have been in famous conflict involving the nondisclosure tort as applied to newspapers, privacy and speech have coexisted harmoniously throughout the overwhelming majority of nondisclosure rules, which have never raised constitutional issues. The Supreme Court may have held in favor of press immunity from privacy rules in the *Florida Star/Bartnicki* line of cases, but it does not follow from these cases that nondisclosure rules applied in other circumstances - for example, to nonpress entities engaged in ordinary commercial activity - are constitutionally suspect. First, the Court has made quite clear in each of these cases that its ruling was narrow. Second, because of the importance of both privacy and the First Amendment, the Court has repeatedly declined to address the issue of "whether truthful publication may ever be punished consistent with the First Amendment." Third, all of these cases involve media defendants publishing allegedly newsworthy facts, but the vast majority of nondisclosure rules do not involve media defendants or newsworthy information, although a few high-profile cases may be produced from time to time.

Where, then, do nondisclosure rules fall under current doctrine? If the privacy tort is dead, why is our law filled with nondisclosure rules that we find constitutionally unproblematic, and, indeed, have never envisioned to fall within the scope of the First Amendment? As Schauer might put it, why have we not perceived the constitutional salience of other nondisclosure rules like the attorney-client privilege or the Video Privacy Protection Act? Some privacy scholars have proffered the concept of "private speech" as a justification for sustaining nondisclosure rules against the First Amendment. Building upon Warren and Brandeis's distinction between matters of public and matters of private interest, these scholars suggest that courts should develop a category of speech that is "private" or at least not a matter of public concern. By so doing, these scholars hope to rejuvenate the tort of disclosure of private facts to make it applicable in at least egregious cases against media defendants. Although the Supreme Court has declined to hold categorically whether truthful speech on a matter not of public concern may ever be restrained consistent with the First Amendment, the "private speech" theory has some support in First Amendment doctrine. For example, in *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, a plurality of the Court noted in a private-figure trade libel case that speech not on matters of public concern receives "less stringent" First Amendment protection. Even in

Bartnicki v. Vopper, a case received gloomily by most privacy scholars, the Court strongly implied that the First Amendment could only defeat privacy if the speech being regulated was "unquestionably a matter of public concern." However, such a theory is mostly unhelpful to the protection of the vast majority of consumer data privacy laws for a couple of reasons. First, by attempting to justify privacy rules against media disclosures, it lumps the easy case of consumer privacy rules with the hard case of privacy against the press. In so doing, it necessarily concedes that privacy rules are speech rules. Second, requiring courts to determine whether speech is "public" or "private" would be incredibly difficult and likely lead to indeterminate and inconsistent outcomes.

It is not necessary to develop a new jurisprudence of private speech to sustain consumer privacy rules, as existing doctrine is more than adequate to protect such rules without implicating the First Amendment. With the historical context of privacy and speech in mind, I believe that two additional factors help explain not only why consumer privacy rules have not been thought to implicate the First Amendment, but also why such rules do not in fact do so. First, many forms of nondisclosure rules are enforceable through express or implied contracts. Second, generally applicable law can operate to create a kind of "information contraband" to which nondisclosure obligations can be attached without encroaching upon the scope of the First Amendment.

....

Contract as a basis for nondisclosure rules is an uncontroversial proposition in the privacy literature, even among the First Amendment critics. n301 Two parties can create an information nondisclosure contract that the courts will enforce, even if the party agreeing to keep the information secret is a newspaper and the information is newsworthy. The Supreme Court has made clear that there does not even need to be an enforceable contract to hold the media liable for damages under such circumstances. In *Cohen v. Cowles Media Co.*, the Court upheld the application of promissory estoppel principles to allow a plaintiff to recover against a newspaper that had broken its promise of confidentiality to him. The plaintiff had disclosed embarrassing information relating to the state lieutenant governor's prior criminal record in exchange for the newspaper's promise to keep his identity secret. The newspaper then published the allegations along with the plaintiff's name. Writing for the Court, Justice White held that the state's "law of general applicability" of promissory estoppel could be enforced against the newspaper because "generally applicable laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news."

....

Volokh . . . admits that the government can supply default rules to relationships that social convention considers confidential, and he suggests that the U.S. West case was incorrectly decided on this basis. However, this additional concession gives away most of the game, because virtually all nondisclosure rules outside the media context tend to reinforce implicit social conventions of confidentiality - for example, as Volokh recognizes, the Video Privacy Protection Act reflects such a social expectation in requiring video rentals to be kept secret. But once the law can modify a relationship of this sort, it is hard to see where such a principle would stop,

other than to render all default rules constitutional. Moreover, to the extent that law can reinforce social norms, a privacy rule applied to an area where there is no existing social convention of confidentiality could, over time, create new such norms. For example, scholars have argued that this is exactly what FTC regulation of privacy policies achieves in the Internet context. It would also seem to follow under this theory that terms should be able to be supplied to constructive "relationships" as well. Just as the law unremarkably can impose duties of confidentiality upon a lawyer when the client reasonably believes that an attorney-client relationship exists, other duties could be prescribed to regulate the ways in which profiling and marketing companies use sensitive customer data, including massive profile databases. Thus, Volokh's acceptance of implied contracts seems to permit the government to supply a whole range of default rules to any relationship involving privacy that the government thinks reasonable to regulate.

Volokh's second limiting principle is that while default rules may be permissible, mandatory rules violate the First Amendment. . . . But other regimes operate to supply mandatory nondisclosure rules without falling within the scope of the First Amendment. For example, trade secret law places a mandatory obligation on those who come across trade secrets not to disclose them to others, even if the person who comes across the secret has no relationship to the trade secret holder. Similarly, contract law supplies a whole host of mandatory terms in the consumer context in which there is reason to believe that diminished capacity exists; yet these terms do not raise constitutional issues. This includes, for example, the legislative prohibition of certain types of transactions where the bargain itself is thought to be unconscionable. In analogous contexts involving consumer privacy, then, mandatory rules should be equally unproblematic - for example, the Children's Online Privacy Protection Act, which does not give children the right to waive their privacy rights and prohibits companies from collecting information about children without parental consent. Similarly, scholars have noted that many consumers do not understand the technology of the Internet, the legal language of privacy policies, or the nature of the trade in personal information. This ignorance leads to a form of "privacy myopia," in which consumers sell their data too frequently or too cheaply. For example, some consumers who care deeply about privacy nevertheless sell their information bit by bit for frequent flier miles. If a legislature were to conclude that consumers were behaving myopically in information transactions, it could also conclude that consumers are incapable of waiving their privacy rights in the context of such a transaction, just as a legislature might police standard-form contracts or consumer credit transactions in the offline context. In all of these examples, economic policing of the risk of unconscionability would be assessed under the rational basis review reserved for economic regulation generally.

. . . .

Another theory under which a wide variety of nondisclosure rules can be justified outside the scope of the First Amendment is the related concept of "generally applicable law." Cohen . . . stood for the much broader theory that a larger category of generally applicable laws do not violate the First Amendment, at least insofar as they do not place a significant burden upon protected, expressive conduct. In other words, Cohen suggests that "generally applicable laws" comprise a broader category, of which contract is but one doctrinal strand of several. Such a conclusion is confirmed by several other cases. For example, in *Seattle Times Co. v. Rhinehart*,

the Court held that a protective order placed on a newspaper involved in litigation could be applied validly to the newspaper to prevent it from disclosing the contents of newsworthy information it learned as a result of the discovery process. Indeed, extrapolating from *Rhinehart*, *Lucas Powe* - no enemy of the press, to be sure - has argued that "if the press broke into a building and pillaged files - or planted bugs - and later published, then the publication could be taken as insult upon injury," and the press could be subjected to liability for publication of the wrongfully obtained information. Such a principle is fully consistent with *Bartnicki* and the other cases in which the Court invalidated public laws and tort actions that interfered with the media's First Amendment rights, because each of those cases held that the media had lawfully obtained the published information. Read together, these cases suggest that information disclosure rules that are the product of generally applicable laws fall outside the scope of the First Amendment. If information is received by an entity in violation of some other legal rule - whether through breach of contract, trespass, theft, or fraud - the First Amendment creates no barrier to the government's ability to prevent and punish disclosure. This is the case even if the information is newsworthy or otherwise of public concern. In this regard, the information is a kind of contraband, and traffic in it (at least by those with unclean hands) can be regulated.

Volokh argues that such a principle could be used to justify troubling laws in the name of "privacy," such as a law providing that all questions by reporters would carry with them an implicit promise of confidentiality, or a law providing that people who buy a product implicitly promise to give the seller equal space to respond to any negative article they publish about the product, unless the seller consents in writing after being given full disclosure of the true purpose for which the product is being bought.

However, unlike the law upheld in *Cohen*, neither of these examples is really a law of general applicability. Because both laws would have a significant impact upon expressive activity on matters of public concern, they would likely trigger intermediate scrutiny under current doctrine. Additionally, because the media confidentiality law singles the media out for special unfavorable treatment, it would be subjected to strict scrutiny. . . . *Cohen* did not just involve information that was unlawfully obtained, but also undeniably newsworthy information that was disseminated by the press, the latter of which the Court has long recognized as filling an important social function. From a First Amendment perspective, no such equivalently important social function is provided by database companies engaged in the trade in personal data. Indeed, a general law regulating the commercial trade in personal data by database, profiling, and marketing companies is far removed from the core speech protected by the First Amendment, and is much more like the "speech" outside the boundaries of heightened review.