

# Protecting Confidentiality of Research Data through Law

Prepared for Data Confidentiality and Access Workshop

16-17 October 2003

By Henry H. Perritt, Jr.

## I. Introduction

Researchers and policymakers continue to struggle with ways to protect the confidentiality of data collected or held by the federal government while allowing researchers to have access to the data. In 2000, the National Academies held a workshop on, “Improving Access to and Confidentiality of Research Data,”<sup>1</sup> and considered alternative approaches for limiting disclosure risks and facilitating data access. That workshop considered technical approaches such as data alteration, and restricting access to certain researchers. Most of the researchers at that workshop preferred legal restrictions expressed in licensing agreements over technical restrictions.<sup>2</sup> Several participants in the workshop suggested that legal protection should be given priority because through that means, “the probability of disclosure can be decreased without imposing costs on rule-abiding researchers.”<sup>3</sup>

This paper builds upon the foundation laid at the 2000 workshop. It suggests a framework within which the efficacy of legal protections of confidentiality can be evaluated, suggests qualitative standards for evaluating the effectiveness of existing law, and identifies alternative approaches for strengthening legal protections.

The paper begins by evaluating the possibility that federal or state law might compel researchers to disclose confidential data received from federal government sources. It identifies the two kinds of private interests that warrant shielding data from disclosure. It then identifies the sources of law that prohibit disclosure of data identified as confidential by the governmental agency from which it was received.

The paper concludes that legal liability is only a weak protection for data confidentiality because the principal privacy statutes do not recognize private rights of action for wrongful disclosure, and the caselaw under common-law legal theories provides sparse support, at best, for recovery for disclosure. Moreover, difficulties in detection, proof, establishing damages and the high cost of litigation makes it unlikely that victims of wrongful disclosure would seek relief in

---

<sup>1</sup> [hereinafter “2000 Workshop Report”].

<sup>2</sup> Id. at 35.

<sup>3</sup> Id. at 36.

the courts. At least one respected commentator agrees with these shortcomings of existing privacy law.<sup>4</sup>

The most promising ways to afford legal protection against wrongful research disclosure are (1) to require researchers receiving private data to establish internal protections, on pain of contract cancellation and bars to receiving grants in the future,<sup>5</sup> and (2) to put non-disclosure language in license agreements that supports “third-party-beneficiary” recovery by data subjects.

## **II. Possibility of Compelled Disclosure**

When the government holds data, whether or not the data have been disclosed to private researchers, it always is possible that someone could compel disclosure by the government under state or federal Freedom of Information Acts.<sup>6</sup>

In limited circumstances duties to disclose under Freedom of Information Acts may extend to private researchers as well as governmental entities, but even in these circumstances, the likelihood of compelled disclosure under the statutes is not increased by making data available to the researchers: disclosure can be compelled even if the data are not available to private researchers. Indeed, when the Freedom of Information Act requires disclosure, private researchers can use those statutes to force governmental entities to make data available to them.

Moreover, as § IV.D explains, researchers are unlikely to be “agencies” under the Freedom of Information Act, and thus the Act imposes no disclosure duties on them.

## **III. Interests Supporting Confidentiality**

Any analysis of law protecting confidentiality of government data must begin by identifying the interests that justify confidentiality. Some of these interests are private, and some are public.

Despite the absence of a comprehensive framework of privacy law in the United States, virtually all of the initiatives in privacy law recognize the same conflicting interests. Privacy involves four sometimes conflicting interests: the interests of the subject, the interests of custodians of information about the subject, the interests of the government in acquiring information and using it for regulatory or prosecutorial purposes, and the interests of private entities or individuals who want to exploit information about others.

---

<sup>4</sup> See Joel R. Reidenberg, Privacy Wrongs in Search of Remedies, 54 *Hastings J. J.* 877 (2003) [hereinafter “Reidenberg”] (identifying reasons why private litigation is unlikely to provide adequate protection against invasions of data privacy).

<sup>5</sup> See § IV.K.

<sup>6</sup> See § IV.D (description of Freedom of Information Act and analysis of its duties and exemptions).

## **A. Private Interests Justifying Confidentiality**

Two types of private interest support keeping certain types of government data confidential: personal privacy interests, and commercial interests.

### **1. Personal privacy**

Privacy encompasses ideas of autonomy, dignity, personal freedom and control. Obviously, privacy is not an absolute right. For example, commitments to maintain privacy may conflict with free expression (if, for example, that free expression might divulge private information). Societies have asserted a need (and therefore a privilege) to gather and use information about individuals for tax purposes, census purposes, health purposes, and so on; to hold people to their obligations as citizens and to serve them in accordance with their entitlements. Such societal assertions must be balanced against the desirability of the personal right of individuals to know what information about them is being gathered and used so that they can monitor the conformity of that use to law and control any uses beyond those sanctioned purposes.

To illustrate the conflicting pressures, it is instructive to compare disclosure policies for health records with policies for pizza delivery records.<sup>7</sup> There are many users who can legitimately argue for access to patient health records without the specific authorization of the patient. In order to meet a number of social, economic, and health needs, a society may allow access to some parts of health records by public health authorities, health researchers, fraud and abuse investigators, accreditation agencies, and even law enforcement under some circumstances. For pizza delivery records, it may never be appropriate to allow for any non-consensual disclosures because there are no overriding societal needs that justify it.

On the other hand, an individual's privacy interest is likely to be greater in his medical records than in his pizza delivery records. And, the public uproar over unauthorized release of medical records is inevitably much larger than in the case for pizza delivery records. Confidentiality of medical information has also been regarded as a pre-requisite for free and candid discussions between health care professionals and their patients. For these reasons, a culture of resistance to unauthorized disclosure of medical records is common in the health profession.

### **2. Commercial Interests Supporting Confidentiality**

The law also prohibits disclosure and use of certain types of information in certain circumstances in order to protect commercial and economic interests. The most general protection is encompassed by the tort of misappropriation of trade secrets. This tort covers information the possession of which affords a competitive advantage because the information is not generally known to one's competitors. It is unavailable with respect to information that is publicly known, but the law imposes other obligations without regard to whether the information

---

<sup>7</sup> This example is adapted from Computer Science and Telecommunications Board, National Research Council, *Global Networks and Local Values* 137 (2001), a report which the author of this paper helped write.

is publicly known. Copyright, trademark, and patent protection extend to information developed through private effort and investment that would be discouraged if others were able to appropriate the results. They thus serve to provide incentives for creative effort, by allowing those engaged in literary, inventive, and product brand development to appropriate the fruits of their effort with less fear that the public goods they generate will be vulnerable to free riding by others.

Some but not all of these interests are protected by Exemption 4 of the Federal Freedom of Information Act.<sup>8</sup> Exemption 4 recognizes that failure to protect some of these types of commercial interest will discourage persons from making information available to the government in response to government requests or mandates.

### **B. Public Interests Supporting Confidentiality**

Governments, even those embracing the values of democracy and transparency, must conduct certain operations in secret. Free and open internal policy debate may be killed if those advancing unpopular policy positions fear that their positions may become publicly known. The interest in robust internal policy debate justifies a deliberative privilege encompassed by “executive privilege” and by Exemption 5 of the Freedom of Information Act.

National security and law enforcement activities often must be conducted in secret lest foreign adversaries learn the identity and methods of intelligence collection and react by shutting off valuable sources of intelligence, and lest those engaged in criminal activity discover that they are the focus of law enforcement attention and respond by making it more difficult to detect and prove their criminal conduct and/or escape apprehension.

Other public interests operate so as to ensure a level playing field in the economic sphere, and protect investigations of financial institutions, certain geological survey data, and inside information about corporate enterprises which, unless disclosed through certain channels can make it possible for certain investors to gain a windfall by exploiting information not generally known to the investing public. The Patriot Act reinforces certain protections, especially in the foreign intelligence, law enforcement, and financial realms, and adjusts the balance between personal privacy and public agency access, without, however, fundamentally altering the law’s protection of public and private interest justifying confidentiality.

## **IV. Sources of Law Protecting Confidentiality**

The United States does not have a comprehensive legal regime to protect data privacy. While common-law causes of action afford private remedies for various types of invasion of privacy, and several federal statutes recognize privacy interests, most individuals harmed by inappropriate disclosure by researchers of data about them could not obtain legal relief at affordable cost.

---

<sup>8</sup> See § IV.D.2.

This part of the paper briefly describes the legal duties and remedies afforded by major common-law and statutory regimes.

### ***A. Common law invasion of privacy***

The common law recognizes a cluster of four invasion-of-privacy torts.<sup>9</sup> Three of these torts embrace a wrongful-conduct view of privacy, and the fourth recognizes a property concept.

The first privacy tort is intrusion upon seclusion.<sup>10</sup> It imposes liability on an actor who unreasonably intrudes into an area or subject as to which the victim has a reasonable expectation of privacy. If the underlying information is public or if the conduct is not unreasonable, there is no liability under this tort.

Giving publicity to private facts is a second privacy tort.<sup>11</sup> One who publicizes private information widely is prima facie liable under this theory, although the publicity may be privileged. The degree of publicity for this tort is greater than that required for defamation.<sup>12</sup> An element of the tort is that the publicized information not be "of legitimate concern to the public," and this is Constitutionally required.<sup>13</sup> The publicity must be offensive to a reasonable person.<sup>14</sup> The expectation of privacy required for this tort is less than that required for the intrusion tort.<sup>15</sup> The publicity tort category involves the same kinds of conduct that are regulated by the federal Privacy Act.

*Shulman v. Group W Productions, Inc.*<sup>16</sup> involved a television station filming of the Medevac and associated medical treatment of automobile accident victims. The victim sued for intrusion into seclusion and giving unwanted publicity to private facts. The television producers defended on First Amendment grounds. The California Supreme Court concluded that summary

---

<sup>9</sup> Restatement (Second) of Torts § 652A (1977) (summarizing four type of invasion of privacy).

<sup>10</sup> Restatement (Second) of Torts § 652B

<sup>11</sup> Restatement (Second) of Torts § 652D

<sup>12</sup> Restatement (Second) of Torts § 652D cmt. a (noting that publication for defamation only requires disclosure to one third person; publicity for invasion of privacy requires that the matter become public knowledge). *Peacock v. Retail Credit Co.*, 302 F. Supp. 418, 422-23 (N.D. Ga. 1969) (rejecting claim against credit reporting company on invasion of privacy grounds; no physical intrusion, and insufficient publicity because credit report was confidential; and any libel was not claimed within one year statute of limitation; summary judgment for defendant)

<sup>13</sup> Restatement (Second) of Torts §652D(b) (1971).

<sup>14</sup> Restatement (Second) of Torts § 652D cmt. c (showing video of surgical procedure to general public though it was meant only for medical students would qualify, but publicizing private wedding would not).

<sup>15</sup> But see Restatement (Second) of Torts § 652D cmt. b (giving as examples of private facts: sexual relations, family quarrels, humiliating illnesses, intimate personal letters, details of home life, past personal history that one would want to forget).

<sup>16</sup> 955 P.2d 469 (Cal. 1998).

judgment was appropriate as to the claim for publication of private facts but not as to the claim for intrusion.

The court applied the elements for giving publicity to private facts under Restatement § 652D, and held that the newsworthy subject of the broadcast defeated liability under this tort.<sup>17</sup> "Under California common law the dissemination of truthful, newsworthy material is not actionable as a publication of private facts."<sup>18</sup>

The intrusion tort, said the court, "best captures the common understanding of an invasion of privacy. ...it is in the intrusion cases that invasion of privacy is most clearly seen as in a front to individual dignity."<sup>19</sup> The court held that the plaintiffs had no reasonable expectation of privacy at the accident scene or that members of the media would be excluded or prevented from photographing the scene. On the other hand, triable issues of fact existed on whether plaintiffs had an objectively reasonable expectation of privacy in the interior of the rescue helicopter, which served as an ambulance.<sup>20</sup> Also, the plaintiffs were entitled to privacy in their conversations with medical rescuers which may have been intruded upon by placing a wireless microphone on one of the medical personnel. The jury was entitled to decide the question of reasonable expectation and offensiveness of the intrusion by the news gatherers.<sup>21</sup>

It suggested that First Amendment protection for news gathering is far narrower than the protection surrounding the publication of truthful material. "Newsworthiness," as we stated earlier, is a complete bar to liability for publication of private facts and is evaluated with a high degree of deference to editorial judgment. The same deference is not due, however, when the issue is not the media's right to publish or broadcast what they choose, but their right to intrude into secluded areas or conversations in pursuit of publishable material. At most, the constitution may preclude tort liability that would place an impermissible burden on news gatherers, depriving them of their indispensable tools.<sup>22</sup>

In *Michaels v. Internet Entertainment Group, Inc.*,<sup>23</sup> a couple obtained a preliminary injunction against display on the Internet of a videotape depicting them engaging in sexual intercourse. They held copyright in the videotape. The district court found requisite probability of success on the merits of both the copyright and invasion of privacy claims, supporting its

---

<sup>17</sup> 955 P.2d at 478.

<sup>18</sup> 955 P.2d at 479 (extensively reviewing case law on First Amendment considerations).

<sup>19</sup> 955 P.2d at 489-490 (applying Restatement (Second) of Torts § 652B).

<sup>20</sup> 955 P.2d at 490.

<sup>21</sup> 955 P.2d at 493.

<sup>22</sup> 955 P.2d at 496 (internal quotations and citations omitted).

<sup>23</sup> 5 F. Supp. 2d 823 (C.D. Cal. 1998).

issuance of a preliminary injunction.<sup>24</sup> The court found likelihood of success on the merits for violation of the California common law and statutory right to publicity,<sup>25</sup> giving publicity to private facts (rejecting the argument that the plaintiffs had opened their lives by other displays of intimate acts),<sup>26</sup> the court also rejected the argument that an earlier display of the tape on the Internet defeated the publicity tort because it rendered the facts no longer private.<sup>27</sup> Obviously no intrusion tort was made out because the plaintiffs had voluntarily performed for the videotape.

The publicity tort will produce liability in research context for someone who takes information of limited circulation that pertains to an individual ("private facts") and significantly increases its circulation.<sup>28</sup>

False-light invasion of privacy<sup>29</sup> is similar to defamation.<sup>30</sup> This theory imposes liability on one who publicizes information in a way that creates false perceptions of the subject of the information. It is not necessary that the original information be private; nor is it necessary that the false impressions in the audience injure reputation in the same way that is necessary for defamation liability.<sup>31</sup> A common example of liability under this tort category is publishing information about a Democratic ward leader causing the public to perceive that she is a Republican. Falsely saying that someone is a Republican is not defamatory, but such false communication may produce liability under this invasion of privacy tort.<sup>32</sup> Liability is imposed, however, only for publicity that would be offensive to a reasonable person.<sup>33</sup>

---

<sup>24</sup> 5 F. Supp. 2d at 828.

<sup>25</sup> 5 F. Supp. 2d at 838.

<sup>26</sup> 5 F. Supp. 2d at 840 (citing Restatement Second of Torts § 652 D Cmt. h).

<sup>27</sup> 5 F. Supp. 2d at 841.

<sup>28</sup> See *Houghton v. New Jersey Manufacture's Insurance Co.*, 615 F. Supp. 299, 307 (E.D. Pa. 1985) (claim for invasion of privacy/disclosure of private facts for investigative report disclosed to insurance company in support of its litigation position failed because of insufficient publication); *Beverly v. Reinert*, 606 N.E.2d 621, 626 (Ill. App. 1992) (affirming dismissal of claim for disclosure of private facts because of possibility that fax message could be intercepted by third parties; although Kentucky law permits disclosure claim to be based on disclosure to one significant person, mere possibility of interception of fax message by unidentified third parties insufficient to state claim)

<sup>29</sup> Restatement (Second) of Torts § 652E.

<sup>30</sup> Restatement (Second) of Torts § 652E cmt. b

<sup>31</sup> Restatement (Second) of Torts § 652E cmt. b. 26 Restatement (Second) of Torts § 652E illus. 4.

<sup>32</sup> Restatement (Second) of Torts § 652E cmt. c (publishing erroneous but not derogatory facts about musician would not be tortious, but falsely placing ones picture in a police "rogues galary" over protest would be).

<sup>33</sup> 28 Restatement (Second) of Torts § 652C

False light liability is likely under circumstances similar to those that would produce liability for under common law defamation doctrines or under data-accuracy statutes. If a database provider maintains information about individuals and the information is inaccurate, liability under this tort probable when the provider disseminates the information. A researcher might face liability under this privacy tort for disclosing data that supports inaccurate inferences about the subject, say information about a false positive HIV test, without disclosing the results of a subsequent test that shows the subject to be free of the HIV virus.

The fourth privacy tort is appropriation of name or likeness.<sup>34</sup> It is the only one of the four privacy categories that has a property flavor. It imposes liability on one who uses the name, image, and possibly other uniquely identifying information about another, for the commercial purposes of the actor. The Restatement commentary says that liability may be imposed for non-commercial appropriation as long as it is for the purpose and benefit of the actor.<sup>35</sup>

Appropriation of name or likeness is unlikely to be important in the research data context unless it is expanded to overlap significantly with trademark and fair competition concepts.<sup>36</sup> Without expansion, this tort would produce liability in the rare situation in which a wrongdoer misappropriates and uses a digitized image or a personal profile of an individual for the wrongdoer's own commercial purposes to trade on the reputation of the subject—for example, selling Ben Affleck's private cellphone number.

One of the major uncertainties with respect to all four invasion-of-privacy torts is whether corporations enjoy protectable privacy interests.<sup>37</sup>

Establishing one or more of the privacy torts entitles the plaintiff to damages and, on appropriate facts, to injunctive relief.

## ***B. Third party beneficiary contract action***

Data subjects injured by disclosure of information about them in violation of a contract (such as a license agreement) between a researcher and a government grantor might be able to

---

<sup>34</sup> Restatement (Second) of Torts § 652C.

<sup>35</sup> Restatement (Second) of Torts § 652C cmt. b.

<sup>36</sup> See *Estate of Boyer v. Docusearch, Inc.*, 816 A.2d 1001, 1009 (N.H. 2003) (rejecting claim for misappropriation of name or likeness; defendant sold personal information about plaintiff's decedent for value of information itself, not to appropriate decedent's individual fame); but see *Reidenberg* 54 Hastings L.J. at 895 (arguing that *Estate of Boyer* opens the door for successful misappropriation claims).

<sup>37</sup> Compare *Fibreboard Corp. v. Hartford Accident & Indemnity Co.*, 20 Cal.Rptr.2d 376, 391 (Cal.App. 1993) (citing Restatement (Second) of Torts § 652I in support of proposition that corporations and partnerships have no protectible interest in privacy) and *N.O.C., Inc. v. Schaefer*, 484 A.2d 729, 730 (N.J.Super. 1984) (following Restatement and denying invasion of privacy cause of action to corporation except for appropriation claim) and *Wadman v. State*, 1993 WL 542374 (Neb. App. 1993) (quoting Nebraska Stat. 20-204, which protects only natural persons against false light invasion of privacy).

recover damages as “third-party beneficiaries” of the contract. In order to recover, they would have to demonstrate that they are intended beneficiaries of the contracts.<sup>38</sup>

As examples (outside the research context), Suppose “A, the operator of a chicken processing and fertilizer plant, contracts with B, a municipality, to use B's sewage system. With the purpose of preventing harm to landowners downstream from its system, B obtains from A a promise to remove specified types of waste from its deposits into the system. C, a downstream landowner, is an intended beneficiary under Subsection (1)(b).”<sup>39</sup>

Or, suppose “A, a labor union, enters into a collective bargaining agreement with B, an employer, in which B promises not to discriminate against any employee because of his membership in A. All B's employees who are members of A are intended beneficiaries of the promise.”<sup>40</sup>

Because there is no apparent reason for a government grantor to impose limitations on data disclosure by a research grantee except to protect the privacy of data subjects, this intended-beneficiary requirement might be relatively easy to satisfy.

A third-party contract beneficiary can recover damages for breach of contract and may be entitled to an injunction when he can demonstrate unique harm.

### ***C. Federal Privacy Act***

The federal Privacy Act covers federal agency records. The scope of the Privacy Act is determined in large part by its definition of record: “any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph.”<sup>41</sup> Because records are covered only if they contain a specific identifying element a mere aggregation of information about

---

<sup>38</sup> Compare Restatement (Second) of Contracts § 302 (1981) (criteria for third-party beneficiary status) with *FDIC v. United States*, 342 F.3d 1313 (Fed. Cir. 2003) (denying third-party beneficiary status to shareholders; contract between government and corporation of which they were shareholders was not intended to benefit them)

<sup>39</sup> Restatement (Second) of Contracts § 302 illus. 10, (1981).

<sup>40</sup> Restatement (Second) of Contracts § 302 illus. 14 (1981). See also *Airplane Sales International Corp. v. United States*, 54 Fed.Cl. 418, 421 (2002) (purchaser of aircraft parts from museum was third party beneficiary of contract between government and museum providing for transfer of aircraft parts to museum and could maintain action for breach of contract to transfer parts).

<sup>41</sup> 5 U.S.C. § 552a(a)(4).

transactions or environmental conditions is not covered even though it may substantially identify an individual.<sup>42</sup>

The Privacy Act forbids disclosure of any record without the written consent of an individual to whom the record pertains<sup>43</sup> unless the disclosure is for the purpose which is compatible with the purpose for which the data was collected.<sup>44</sup> It mandates disclosure to the subject of a record upon his request.<sup>45</sup> It mandates an accurate accounting of all disclosures and corrections,<sup>46</sup> and requires the agency to accept "statements of disagreement" from subjects challenging a refusal to amend a record to correct an alleged inaccuracy.<sup>47</sup> The statute also prohibits agencies from maintaining records other than those "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the president."<sup>48</sup> It obligates agencies to maintain records with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual"<sup>49</sup> in determination made based on the records.<sup>50</sup> Agencies must make reasonable efforts to notify subjects when records about them are disclosed under compulsory process.<sup>51</sup> Agencies also must establish appropriate administrative, technical, and physical safeguards to insure security and confidentiality and to protect records against anticipated threats to their integrity.<sup>52</sup>

---

<sup>42</sup> In theory, one could establish a record with detailed geographic information, and temporal information that would identify an individual because she was the only one standing in a particular place at a particular time.

<sup>43</sup> 5 U.S.C. § 552a(b).

<sup>44</sup> Subsection (b)(3) is an exception to the general prohibition against disclosure without written permission and is linked to the definition of routine use in subsection (a)(7), which is defined with respect to the purpose for which the record data was collected.

<sup>45</sup> 5 U.S.C. § 552a(d).

<sup>46</sup> 5 U.S.C. § 552a(c). The accounting must be made available to subjects upon their request. 5 U.S.C. § 552a(c)(3)

<sup>47</sup> 5 U.S.C. § 552a(d)(2)-(4).

<sup>48</sup> 5 U.S.C. § 552a(e)(1).

<sup>49</sup> Compare *Sellers v. Bureau of Prisons*, 959 F.2d 307, 312 (D.C. Cir. 1992) (adverse determinations supported by unchecked information results in civil liability if agency could have verified accuracy; reversing district court) with *Johnston v. Horne*, 875 F.2d 1415, 1422 (9th Cir. 1989) (inaccurate background briefing supporting involuntary retirement was grossly negligent but did not violate Privacy Act, which imposes liability only for willful or intentional conduct).

<sup>50</sup> 5 U.S.C. § 552a(e)(5).

<sup>51</sup> 5 U.S.C. § 552a(e)(8).

<sup>52</sup> 5 U.S.C. § 552a(e)(10).

Federal contractors as well as federal agencies may be subject to obligations imposed by the Privacy Act. Subsection (m)(1) provides that, "when an agency provides by contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. . . ." <sup>53</sup> This effectively obligates the agency to impose contractual obligations on its contractors when they operate "systems of records." In addition, the same subsection continues, "for purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency." <sup>54</sup> This directly imposes statutory obligations and affords statutory remedies with respect to contractor conduct within the scope of subsection (i). Subsection (i) imposes criminal penalties on agency employees (and by virtue of subsection (m) on contractors and their employees) who, knowing of the Privacy Act prohibitions on disclosure of specific material, nevertheless willfully disclose it to someone not entitled to receive it. <sup>55</sup>

Federal contractors and grantees are not likely to be subject to the Privacy Act in the usual research context, because they are not likely to be government contractors within subsection (m). The phrase "when an agency provides by contract for the operation . . . of a system of records . . . ." might be satisfied, but the omitted language in that quotation "by or on behalf of the agency . . . to accomplish an agency function" would not be satisfied. Suppose the agency is the NSF. That agency's function is the sponsorship of research and development. A grantee receiving data held by the government to perform sponsored research would not be performing the agency's function. The best interpretation of subsection (m) is that it is aimed at ensuring that agencies cannot evade their obligations under the Privacy Act by delegating internal agency functions to private contractors. That is not what the NSF has done when it sponsors applied research and discloses data in conjunction with that research, and therefore the research grantees should not be within the ambit of subsection (m). <sup>56</sup>

Injunctions against release of information covered by the Privacy Act are not available, <sup>57</sup> but the criminal penalties imposed by the Act may deter violations.

#### ***D. FOIA and its exemptions***

The Freedom of Information Act <sup>58</sup> extends to virtually all records held by federal agencies outside the judicial and legislative branches of government, including electronic

---

<sup>53</sup> 5 U.S.C. § 552a(m)(1).

<sup>54</sup> 5 U.S.C. § 552a(m)(1).

<sup>55</sup> 5 U.S.C. § 552a(i).

<sup>56</sup> Cf. *Dong v. Smithsonian Institution*, 125 F.3d 877 (D.C. Cir. 1997) (Smithsonian Institution was not "agency" subject to Privacy Act).

<sup>57</sup> *Cell Associates, Inc. v. National Institutes of Health*, 579 F.2d 1155, 1159 (9<sup>th</sup> Cir. 1978)

formats. FOIA is interpreted broadly, and its exemptions narrowly.<sup>59</sup> The purpose for which one requests an agency record under FOIA is irrelevant.<sup>60</sup>

The following types of information are exempt from FOIA disclosure:

- (1)** (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
- (2)** related solely to the internal personnel rules and practices of an agency;
- (3)** specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (4)** trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (5)** inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (6)** personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (7)** records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (8)** contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (9)** geological and geophysical information and data, including maps, concerning wells.<sup>61</sup>

---

<sup>58</sup> 5 U.S.C. § 552 (2003).

<sup>59</sup> See *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151-52 (1989) (reiterating basic principle but finding that records requested by defense contractor were properly withheld because within law enforcement exemption even though not originally created for law enforcement purposes); *United States Department of Justice v. Tax Analysts*, 492 U.S. 136, 142 n.3 (1989) (burden on agency to show that requested records not within FOIA); *Assembly v. United States Department of Commerce*, 968 F.2d 916, 920 (9th Cir. 1992) (reiterating pro-disclosure policy of FOIA and affirming order that Commerce Department disclose computer tapes with census figures).

<sup>60</sup> 5 U.S.C. § 552 (a)(4)(a)(ii)(1994)(providing that agency regulations must develop fees schedules for both commercial and private use).

<sup>61</sup> 5 U.S.C. §552(b) (2003).

These exemptions are construed narrowly.<sup>62</sup> It is important to understand that coverage by an exemption is not the same thing as a prohibition on disclosure; an agency generally is free to disclose whatever it wants, consistent with the Privacy Act and other statutes. Coverage by an exemption simply means that an agency is not *compelled* to disclose the information.

In *Chrysler Corp. v. Brown*,<sup>63</sup> the Supreme Court held that injunctions are available to block disclosure under the Freedom of Information Act, when the person opposing disclosure can show that an agency's decision to disclose was "arbitrary and capricious" or was based on a misinterpretation of FOIA or other federal law.<sup>64</sup>

## 1. Exemption 6 – personal privacy

The scope of the privacy exemptions to the FOIA usually depends on whether the invasion of privacy is "unreasonable" or "unwarranted." To apply this standard, a decisionmaker must consider the interests of the requester to determine whether they should override the interests of the subject.<sup>65</sup>

For example there is much uncertainty over whether certain types of publicly held information, collected from private individuals, and containing personal information, such as drivers' license records, should be subject to disclosure under freedom of information laws. In *Department of Defense v. Federal Labor Relations Authority*,<sup>66</sup> The Supreme Court restricted release of personal data, balancing privacy interests against what it understood to be the "core purposes" of the FOIA. "[T]he only relevant "public interest in disclosure" to be weighed in this

---

<sup>62</sup> *Anderson v. Department of Health and Human Services*, 907 F.2d 936, 941 (10th Cir. 1990) (FOIA exemptions must be construed narrowly and agency asserting exemption has burden of proof).

<sup>63</sup> 441 U.S. 281 (1979).

<sup>64</sup> *Id.* at 318-319.

<sup>65</sup> See *United States Dep't. of Defense v. Fed. Labor Relations Auth.*, 114 S.Ct. 1006, 1012 (1994) (to decide whether a record is exempt from FOIA disclosure under Exemption 6, court must "balance the public interest in disclosure against the interest Congress intended the exemption to protect" in order to decide whether the invasion of privacy would be "unwarranted")(quoting *Department of Justice v. Reporters Comm. for Freedom of Press*, 489 US 749, 773 (1989); *United States Department of State v. Ray*, 502 U.S. 164, 178, 112 S.Ct. at 549 (1991) (balancing privacy against basic policy of FOIA; official information that sheds light on an agency's performance of its statutory duties falls squarely within FOIA's purpose); *United States Dep't. of Justice v. Reporters' Comm. for Freedom of the Press*, 489 U.S. 749, 771-72 (1989) (whether invasion of privacy is warranted cannot turn on purposes for which the request for information is made, but whether disclosure of private document under Exemption 7(C) is warranted must turn on nature of requested document and its relationship to "basic purpose of FOIA; basic purpose not served by disclosure of information about private citizens accumulated in various government files that reveals little or nothing about agency's own conduct); *Minnesota Medical Association v. State*, 274 N.W.2d 84 (Minn. 1978) (data requested by publishing company regarding abortions performed for medical assistance recipients not exempt for privacy reasons); *State ex rel. Stephan v. Harder*, 641 P.2d 366 (Kan. 1982) (disclosure of information on abortions performed by physicians receiving public funds did not threaten physician privacy rights).

<sup>66</sup> 510 U.S. 487 (1994).

balance is the extent to which disclosure would serve the "core purpose of the FOIA," which is "contribut[ing] significantly to public understanding of the operations or activities of the government. [FOIA's] basic policy of 'full agency disclosure unless information is exempted under clearly delineated statutory language,' indeed focuses on the 67 citizens' right to be informed about what their government is up to. Official information that sheds light on an agency's performance of its statutory duties falls squarely within that statutory purpose. That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct."<sup>68</sup>

Justice Ginsburg disagreed. "The Reporters Committee "core purpose" limitation is not found in FOIA's language. A FOIA requester need not show in the first instance that disclosure would serve any public purpose, let alone a "core purpose" of "open[ing] agency action to the light of public scrutiny" or advancing "public understanding of the operations or activities of the government."<sup>69</sup>

In *Campaign for Family Farms v. Glickman*,<sup>70</sup> the Court of Appeals affirmed an injunction against release by USDA of the names and addresses of some 19,000 persons signing a petition to alter a program for collecting money for marketing and advertising of pork. The court held that the signers enjoyed a privacy interest in a secret ballot (the petition recited how the signers would vote), and that their limited disclosure to each other and to the USDA did not waive their privacy rights. It further held that the public interest in disclosure was slight, because the only entity wishing to know the contested information was the association representing pork producers whose interests in the marketing and advertising program were antagonistic to those of the people signing the petition.

## 2. Exemption 4 – commercial information

In order for information to be within exemption 4, it must be either a trade secret or (1) commercial or financial information, (2) obtained from a person, and (3) privileged or confidential. Commercial or financial information is confidential for purposes of the exemption if its disclosure will likely (a) impair the government's ability to obtain necessary information in the future or, (b) cause substantial harm to the competitive position of the person from whom the information was obtained.<sup>71</sup> Exemption 4 applies only when an agency (usually assisted by the

---

<sup>67</sup> 510 U.S. at 494.

<sup>68</sup> 510 U.S. at 494-496 (internal quotations and citations omitted).

<sup>69</sup> (Ginsburg, J., dissenting)

<sup>70</sup> 200 F.3d 1180 (8<sup>th</sup> Cir. 2000),

<sup>71</sup> *Miami Herald Pub. Co. v. United States Small Business Administration*, 670 F.2d 610, 613-614 (5<sup>th</sup> Cir. 1982) (insufficient showing of competitive harm).

originator of the information) can show that competitive harm to the originator would result from disclosure.<sup>72</sup>

### 3. Application in research context

Application of Federal FOIA in the government-research-contract context is challenging. Three types of information present special problems in striking the appropriate balance between transparency and privacy values. The first is scientific and technical data developed by persons employed outside the government in academic and research institutions. When their work is supported by public financing, expansive interpretations of freedom of information laws may make their work publicly accessible even before they draw final conclusions based on the data. Such FOIA coverage, although it is supported by arguments that the public should have free access to data generated with public funds, presents two problems. Disclosure of the data may compromise privacy interests of data subjects, and it may negate legitimate expectations of intellectual property protection for the researchers.

Second, proprietary information originating with third parties often is submitted to public authorities in response to legal requirements or in support of applications or licenses or other benefits. When such third party information is disclosed under freedom of information law, difficult copyright and trade secrets issues must be addressed. Disclosure under a freedom of information law does not extinguish any copyright held by the third party,<sup>73</sup> but it may extinguish trade secrets.<sup>74</sup>

Third, personal information often is submitted to public authorities in response to legal requirements or in support of applications for benefits such as drivers licenses or social welfare payments. This information is at the core of personal privacy exemptions included in virtually all existing freedom of information law or proposals.

But these difficult policy issues are largely insulated from judicial review. Government contractors and grantees are not, generally speaking, “agencies” covered by the FOIA.<sup>75</sup> Moreover, government contracts can be structured so that an agency lacks control over some or all of the information. When that occurs, is the information an “agency record” involved within

---

<sup>72</sup> See *GC Micro Corp. v. Defense Logistics Agency*, 33 F.3d 1109, 1115 (9<sup>th</sup> Cir. 1994) (insufficient showing; disclosure appropriate).

<sup>73</sup> See §IV.H.

<sup>74</sup> See § IV.H.2.

<sup>75</sup> *Public Citizen Health Research Group v. Department of Health, Ed. and Welfare*, 668 F.2d 537, 543 544 (D.C. Cir. 1981) (medical foundation under contract to serve as professional standards review organization was not “agency” under FOIA); *Forsham v. Harris*, 445 U.S. 169, 178-179 (1980) (federal funding did not make data collected and retained by grantee agency “records” subject to FOIA; nor was grantee “federal agency”); *Lombardo v. Handler*, 397 F.Supp. 792, 802 (D.D.C. 1975) (National Academy of Sciences was not “agency” within FOIA; FOIA does not apply to private entities that contract with government to conduct studies), affirmed 546 F.2d 1043 (D.C. Cir. 1975)

the meaning of FOIA? In *Tax Analysts v. United States Department of Justice*<sup>76</sup> the district court held that the requested information did not constitute agency records within FOIA because, under the terms of the contract between the government and West Publishing, the government did not have “control” of the information.<sup>77</sup>

### **E. Census Statutes**

Section 9(a) of the Census Act,<sup>78</sup> prohibits disclosure of census information that can identify an individual. The Act imposes penalties on federal employees who violate its prohibitions, but has not been construed to afford private persons standing to sue to enforce it.<sup>79</sup>

### **F. 18 U.S.C. § 1905**

Section 1905 of Title 18, United States Code provides:

“Whoever, being an officer or employee of the United States or of any department or agency thereof . . . publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency . . . which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.”<sup>80</sup>

In *Chrysler Corp. v. Brown*,<sup>81</sup> the United States Supreme Court held that the statute does not authorize a private right of action to enforce it.<sup>82</sup>

### **G. Fourth Amendment**

The Fourth Amendment to the United States Constitution reads:

---

<sup>76</sup> *Tax Analysts v. U. S. Dept. of Justice*, 913 F. Supp. 599, 604-605 (D.D.C. 1996)

<sup>77</sup> *Tax Analysts v. U. S. Dept. of Justice*, 913 F. Supp. 599, 604-605 (D.D.C. 1996)

<sup>78</sup> 13 U.S.C. §9(a) (2003).

<sup>79</sup> *St. Regis Paper Co. v. U.S.*, 368 U.S. 208 (1961).

<sup>80</sup> 18 U.S.C. § 1905 (2003).

<sup>81</sup> 441 U.S. 281 (1979).

<sup>82</sup> 441 U.S. at 316-317.

"The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures shall not be violated, and no warrant shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."<sup>83</sup>

The Fourth Amendment only protects against searches by officers of the state, and not purely private searches no matter how unreasonable.<sup>84</sup> It does not limit disclosure of information.

## ***H. Intellectual property***

Owners of intellectual property rights in data possessed by researchers can enforce those rights regardless of how the researchers obtained the data. For example, disclosure of information under the FOIA does not extinguish copyright. So, one might be entitled to compel the government to disclose copyrighted information, but still be liable to the owner of the copyright for subsequent reproduction or public dissemination. Other forms of intellectual property such as trade secret, patent, and trademark, are worth considering, but are unlikely to be implicated in researcher disclosure, absent unusual circumstances.

### **1. Copyright**

A copyright is a property interest embodied in the tangible representation<sup>85</sup> of information. Copyright is a limited property interest. The most important limitation is that, unlike interests in real property and unlike interests conferred by patents, copyright does not give the owner the right to exclude all uses of the property. Rather, a copyright owner may exclude only certain uses, those defined in § 106: copying, distributing, preparing derivative works, and displaying or performing publicly.<sup>86</sup>

Even if conduct by a user of a work or a producer of added value invades a right exclusively reserved to a copyright owner, the conduct nevertheless may be privileged by the fair use doctrine.<sup>87</sup> There are four statutory factors to be considered in evaluating an assertion of fair

---

<sup>83</sup> U.S. Const. Amdt. IV.

<sup>84</sup> *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1112 (D. Kan. 2000) (search of computer files by Internet service provider did not violate the Fourth Amendment because accomplished entirely by private individuals).

<sup>85</sup> Protecting only tangible representations results from the fixation requirement of 17 U.S.C. § 102(a).

<sup>86</sup> 17 U.S.C. § 106 (2003) (certain of the rights are associated only with particular kinds of works; those limitations are not material to the discussion).

<sup>87</sup> 17 U.S.C. § 107 (2003) (codifying fair use and identifying factors).

use,<sup>88</sup> but the four factors are not exclusive; rather, they are the starting point for a broad equitable inquiry.<sup>89</sup> The impact on markets for the underlying work, the fourth statutory factor, is the most important.

In *Feist Publications v. Rural Telephone Co.*,<sup>90</sup> the Supreme Court of the United States eliminated the possibility of copyright protection for “sweat of the brow” - the effort in assembling factual information -- except when the selection and arrangement of such information involves nontrivial creative contributions. In no event can copyright extend to the underlying factual information. For example, *Feist* does not permit a copyright in survey information or basic records of land ownership.<sup>91</sup> The *Feist* analysis proceeds from the proposition that facts may not be copyrighted because they lack the originality component that is constitutionally mandated as a prerequisite for copyright.<sup>92</sup> The basic lesson of *Feist* is that one who assembles factual data, even at great effort and cost, is not entitled to copyright in the basic data.

*Feist* does not eliminate the possibility of extending copyright protection to value added enhancements, say by creative data transformations. But the *Feist* court specifically rejected the idea that originality can result simply from gathering facts. It rejected “sweat of the brow” justification for copyright. Moreover, even copyrighted compilations are copyrightable only to the extent of their original selection or arrangement. “[A] subsequent compiler remains free to use the facts contained in another’s publication to aid in preparing a competing work, so long as the competing work does not feature the same selection and arrangement.”<sup>93</sup>

---

<sup>88</sup> 17 U.S.C. § 107(1) (purpose and character of use); id. § 107(2) (nature of copyrighted work); id. § 107(3) (amount and substantiality of material used relative to copyrighted work); id. § 107(4) (effect of use on potential market for or value of copyrighted work).

<sup>89</sup> See *Sony Corp. v. Universal Studios*, 464 U.S. 417 (1984).

<sup>90</sup> 499 U.S. 340 (1991).

<sup>91</sup> See *Mason v. Montgomery Data, Inc.*, 765 F.Supp. 353, 355 (S.D.Tex.,1991) (factual matters such as the abstract, tract boundaries and ownership name and tract size are not copyrightable). The court of appeals reversed, 967 F.2d 135 (5th Cir. 1992), holding that the district court had erroneously found that the merger doctrine barred copyright of the plaintiff’s maps. The district court found that the maps were the only pictorial presentation which could result from a correct interpretation of the legal description and other uncopyrightable facts. Id. at 138 (characterizing district court conclusion). The court of appeals disagreed, finding that the underlying data could be portrayed in a variety of ways. Id. at 139. Thus, under the merger doctrine, the plaintiff’s portrayal in its maps could be protected without preempting free use of the underlying facts. Id. (explaining motivation for merger doctrine and noting how competing maps differ in selection of sources, interpretation of sources, discretion in reconciling inconsistencies and skill and judgment in depicting information). The court, disagreeing with the defendants, found that *Feist*’s standards for selection, coordination and arrangement pertain to application of the merger doctrine, as well as to the threshold question of originality. Id. at 140 n.7. The court went on also to find that the plaintiff’s added value satisfied the requirements for originality. Id. at 141.

<sup>92</sup> 499 U.S. at 347-48.

<sup>93</sup> 499 U.S. at 349.

Under *Feist*, it is extremely unlikely that raw data disclosed to researchers would be protected by copyright.

## 2. Trade Secret

Trade secret affords the developer of useful commercial information that the developer keeps secret with a tort remedy against anyone who wrongfully obtains and uses the trade secret.

Almost any subject matter can qualify as a trade secret if the requisite secrecy and competitive advantage (discussed in this section) exist. Formulas for products, production processes, marketing techniques, customer information, supplier information, and financial practices all qualify. More important than type of subject matter is secrecy. Knowledge cannot be a trade secret unless it is secret. While owners of trade secrets may disclose the secret to employees, suppliers, customers, and in negotiations, it is essential that such disclosures be shielded either by special relationships or by explicit contractual undertakings limiting further disclosure and use.

Trade secret regulation, unlike patent, copyright, and trademark law, is primarily a creature of state law, increasingly regularized by adoption of the Uniform Trade Secret Act.

A trade secret is

1. information used in a business
2. that is secret, and
3. that gives economic advantage to the person with knowledge of it

Trade secret misappropriation protects only secret information that affords a competitive advantage because it is secret. A plaintiff must show that the information was not in the public domain and that the owner of the alleged trade secret took reasonable measures to maintain its secrecy. The requirement that economic advantage flow from the trade secret is closely associated with the secrecy requirement and does not necessarily represent a conceptually independent element, unlike the novelty element in patent law.

Contracts can reinforce trade secret protection by permitting one supplier to disclose a trade secret to the suppliers of other types of added value without losing the secrecy that is a requisite of trade secret status. Such a contract imposes appropriate restrictions on redisclosure. For example a contract could provide access to a trade secret while limiting use of the trade secret only for particular purposes.

Of course, contractual protection only binds parties to the contract. A supplier of information value may have no effective remedy over someone impairing his economic interest

if he has no privity of contract with the actor.<sup>94</sup> The supplier may be able to enforce a contractual restriction on disclosure by his first customer, but if a customer of that customer discloses, the original supplier has no contractual remedy against the second downstream customer because there is no privity between that customer and the original supplier. Of course, the original supplier may require his immediate customer to impose contractual restrictions on its customers but a failure to impose such restrictions is simply a breach of contract by the first customer and creates no right against the subsequent customers not so restricted.

Under the "property" view of trade secret law, the theoretical basis for trade secret misappropriation is not only the breach of a confidential relationship but also the injury to the plaintiff that results from the use of the plaintiff's intellectual property.<sup>95</sup> The property view emphasizes qualification as a trade secret, while the confidential relations view emphasizes the existence of a confidential relationship without regard to the type of information involved.<sup>96</sup>

Misappropriation is the conduct element of trade secret misappropriation and involves:

1. acquisition of a trade secret through the use of improper means,
2. use or disclosure of a trade secret in breach of confidence
3. use or disclosure of a trade secret with actual or constructive knowledge that (a) the trade secret was acquired by improper means, (b) was disclosed in violation of a duty arising out of a special relationship, or (c) was acquired by accident or mistake

Much of the controversy in trade secret cases involves defining the scope of conduct that can lead to the imposition of liability for trade secret misappropriation. Two types of conduct potentially qualify: conduct violating express or implied contractual or fiduciary obligations in the context of a "special relationship," and conduct by a "stranger" constituting "improper means." Bad faith exists in the mind of someone who uses or disclose a trade secret knowing that it was acquired through improper means, knowing that it was disclosed and thus acquired in violation of a special relationship or knowing that it was acquired through accident or mistake.

There are three types of conduct potentially tainted by the three types of mental state. Acquisition is tortious if coupled with a breach of a confidential relationship or improper means.

---

<sup>94</sup> Accord, Jane C. Ginsburg, *Creation and Commercial Value: Copyright Protection of Works of Information*, 90 Colum. L. Rev. 1865, 1920 (1990) (noting the privity limitation on contractual protections).

<sup>95</sup> *Den-Tal-Ez Inc. v. Siemens Capital Corp.*, 566 A.2d 1214, 1228 (Pa. Super. 1989) (en banc) (characterizing Pennsylvania law under *Van Products Co. v. General Welding & Fabricating Co.*, 213 A.2d 769 (Pa. 1965) as rejecting the Holmes confidential relations view).

<sup>96</sup> *Siemens* at 1228.

Disclosure is tortious if coupled with a confidential relationship, knowledge of someone else's breach of a confidential relationship, coupled with improper means or knowledge of someone else's use of improper means.

Use is tortious in the same circumstances that disclosure is.

The owner of a misappropriated trade secret, upon establishing the elements of the tort, can recover damages and usually also is entitled to injunctive relief. The Uniform Trade Secrets Act authorizes injunctions<sup>97</sup> and damages<sup>98</sup> for misappropriation of trade secrets.

A significant limitation of trade secret protection is that the protection is lost when the protected information is disclosed unless the disclosure is accompanied by contractual restrictions. So if a researcher discloses trade secrets obtained from the government, the information ceases to qualify as a trade secret. The owner of the trade secret cannot recover from the researcher unless she can show that the researcher was bound by contract with the government to maintain the trade secret, or otherwise knew that the information was a trade secret.

### 3. Trademark

Trademarks are marks that identify the source of a product or service, such as “Coca-Cola,” “Buick,” and “Microsoft Windows.”<sup>99</sup> Property rights in a trademark are protected only against uses by others that create consumer confusion as to the producer or source of the goods.<sup>100</sup> Under the Lanham Act, the property right in trademarks can be lost through abandonment or non-use,<sup>101</sup> or if the mark becomes so well used that it becomes generic.<sup>102</sup>

---

<sup>97</sup> UTSA § 2.

<sup>98</sup> UTSA § 3.

<sup>99</sup> The Lanham Act, as amended in 1988, defines a trademark as "any word, name, symbol, or device, or any combination thereof -(1) used by a person or (2) which a person has a bona fide intention to use in commerce and applies to register on the principle register established by this chapter, to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown." 15 U.S.C. §1127. The Act also applies to service marks which are defined identically to trademarks with the exception that servicemarks apply to services rather than goods. 15 U.S.C. §1127.

<sup>100</sup> Certain “famous” marks also are protected against “dilution.”

<sup>101</sup> §14 of the Lanham Act, codified at 15 U.S.C. 1064 (3). See generally, 1 J. Thomas McCarthy, Trademarks and Unfair Competition §§17:1 -17:10 (2d ed. 1984).

Federal trademark law has two purposes. First, trademark protection serves to "foster competition and the maintenance of quality by securing to the [owner of the trademark] the benefits of good reputation."<sup>103</sup>

The second purpose of federal trademark law is consumer protection. Affording legal protection to the holder of a trademark ensures that consumers of a product will get what they expect because trademarks encourage manufacturers to maintain consistent quality standards in order to benefit from consumer recognition of their trademark.

Trademark controversies involving data are rare, but they do exist. *United States Golf Association v. St. Andrews Systems, Data-Max, Inc.*<sup>104</sup> is an example. The case involved a claim by an amateur golf association that a computer company had misappropriated its handicapping formula and falsely represented its origin, in violation of the common law and the Lanham Act. The court of appeals affirmed denial of an injunction and summary judgment in the defendant's favor because the handicapping formula was functional and thus beyond the protection of the Lanham Act (the federal trademark statute).<sup>105</sup>

Remedies for infringement include injunctions, monetary damages, costs including attorneys fees, and cancellation of trademark registration.

#### **4. Patent**

Patents give the inventors or discoverers of new and useful processes, machines, manufactures and compositions of matter<sup>106</sup> the "right to exclude others from making, using or

---

<sup>102</sup> § 14 of the Lanham Act, codified at 15 U.S.C. 1064 (3). Examples of generic, and therefore unprotectable, terms include Aspirin (Bayer Co. v. United Drug Co., 272 F. 505 (D.C.S.D.N.Y. 1921)), the board game Monopoly (Anti-Monopoly, Inc. v. General Mills Fun Group, Inc., 684 F.2d 1316 (9th Cir. 1982)), and shredded wheat (Kellogg Co. v. National Biscuit Co., 305 U.S. 111 (1938)). See generally, 1 J. Thomas McCarthy, Trademarks and Unfair Competition §12:3 (2d ed. 1984).

<sup>103</sup> *San Francisco Arts & Athletics, Inc. v. U.S. Olympic Committee*, 483 U.S. 522, 531 (1987)(quoting, *Park N' Fly, Inc. v. Dollar Park and Fly, Inc.*, 469 U.S. 189, 198 (1985).

<sup>104</sup> 749 F.2d 1028 (3d Cir. 1984) (Becker, J.)

<sup>105</sup> 749 F.2d at 1029-1030.

<sup>106</sup> 35 U.S.C.. § 101 (2003) (patentable inventions).

selling" the invention,<sup>107</sup> and, to prevent the importation of products made with a patented process.<sup>108</sup>

Unlike other forms of intellectual property, a patent permits the property owner to exclude users of the patented concept even when the users are completely innocent and know nothing of the patented idea.

Patent protection is unlikely to arise in the research-data context because mere information is not patentable subject matter.

## ***I. European Privacy Directive***

The thinness of U. S. data protection law usefully can be contrasted with stronger protection in Europe. In October, 1992, the European Commission issued a revised proposal for a directive from the council of Europe on data protection.<sup>109</sup> The 1992 proposal requires the members of the European Community to enact data protection statutes meeting minimum requirements. It precludes restrictions on movement of data within the community, but restricts the movement of data to countries that do not provide equivalent data protection to that provided under its terms. Member states were expected to come into compliance by July, 1994.<sup>110</sup> The European Parliament reacted adversely to the proposed ban on transfer of personal data from member states with high levels of protection to those with less protection, and requested changes in the Commission proposal.<sup>111</sup> In early March, 1995, the institutions of the European Union adopted a "common position" on the data protection directive.

The European Commission proposal contemplates eight duties:

---

<sup>107</sup> 35 U.S.C. § 271 (2003)(whoever without authority makes, uses or sells any patented invention, within the United States during the term of the patent therefor, infringes the patent).

<sup>108</sup> 35 U.S.C. § 154 (1988).

<sup>109</sup> Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Eur. Comm. Doc. COM(92) 422, final-SYN 287, art. 6(1)(b) (Oct. 15, 1992) [hereinafter "1992 Proposal"]

<sup>110</sup> 1992 proposal, Art. 35, § 1. See generally Patrick E. Cole, New Challenges to the U. S. Multinational Corporation in the European Economic Community: Data Protection Laws, 17 N.Y.U.J. Int'l L. & Pol. 893 (1985) (surveying law in member states and comparing with EC directive).

<sup>111</sup> See Less Stringent EC Data Protection Requested, 4 No. 5 J. Proprietary Rights (Prentice Hall) 31 (April 1992).

1. a data quality duty,<sup>112</sup> including a duty not to engage in negligent processing of data.<sup>113</sup>
2. an advance notice of an intent to collect and maintain data on an individual<sup>114</sup>
3. a duty to disclose data to the subjects upon request<sup>115</sup>
4. a duty to notify subjects of adverse decisions based on data<sup>116</sup>
5. a duty to notify subjects of disclosure to third parties<sup>117</sup>
6. a duty to correct inaccurate data<sup>118</sup>
7. a duty to maintain reasonable security<sup>119</sup>
8. a duty to notify the data authority of certain acts.<sup>120</sup>

The European Directive is unlikely to affect U.S. researchers, except that it might block the flow of data from European sources to U.S. entities.

## **J. HIPPA**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")<sup>121</sup> called for the enactment of health privacy legislation based on recommendations by the Secretary of Health and Human Services. The statute also authorized the secretary of HHS to promulgate health

---

<sup>112</sup> 1992 Proposal Art. 6.

<sup>113</sup> 1992 Proposal Art. 23(1).

<sup>114</sup> 1992 Proposal Art. 11, § 1.

<sup>115</sup> 1992 Proposal Art. 10, § 1.

<sup>116</sup> 1992 Proposal Art. 13 § 5.

<sup>117</sup> 1992 Proposal Art. 12 § 1.

<sup>118</sup> 1992 Proposal Art. 13 § 3.

<sup>119</sup> 1992 Proposal Art. 17.

<sup>120</sup> 1992 Proposal Art. 18 § 1.

<sup>121</sup> Pub. L. 104-191, § 264 (c)(1).

privacy regulations if the Congress did not act. On November 3, 1999, HHS promulgated such regulations.<sup>122</sup>

The regulations prohibit covered entities from using or disclosing individual protected health information except as permitted by the regulations, which include carrying out treatment, payment, and healthcare operations, pursuant to authorizations by the subject.<sup>123</sup> Covered entities must disclose protected health information to subjects, to the Secretary of HHS to facilitate investigations of compliance.<sup>124</sup> The requirements are relaxed when personally identifying information is removed from the records.<sup>125</sup> Certain uses and disclosures of covered information may be made only with individual authorization.<sup>126</sup> These uses include uses for marketing of health and non health items and services by the covered entity, disclosure by sale, rental, or barter, disclosure to non health related divisions of the covered entity for uses in marketing life or causality insurance or banking services, disclosure, prior to an individual's enrollment in a health plan, to the health plan or healthcare provider for making eligibility or enrollment determinations relating to the individual or for underwriting or risk rating determinations, disclosure to an employer for use in employment determinations, and use or disclosure for fundraising purposes.<sup>127</sup> Significantly, "a covered entity may not condition the provision to an individual of treatment or payment on the provision by the individual of a requested authorization for use or disclosure, except where the authorization is requested in connection with the clinical file."<sup>128</sup>

The regulations contain significant exceptions to the authorization requirement, including disclosures for public health activities,<sup>129</sup> disclosures for health oversight activities including audits, investigations, inspections relating to healthcare systems,<sup>130</sup> disclosures to coroners and medical examiners<sup>131</sup> and disclosures to law enforcement officials.<sup>132</sup>

---

<sup>122</sup> 64 Fed. Reg. 59918 (Nov. 3, 1999), codified at 45 C.F.R. §§ 164.500-164.534 (2003).

<sup>123</sup> 45 C.F.R. § 164.506.

<sup>124</sup> 45 C.F.R. § 164.506 (a)(2).

<sup>125</sup> 45 C.F.R. § 164.506 (d).

<sup>126</sup> 45 C.F.R. § 164.508.

<sup>127</sup> 45 C.F.R. § 164.508 (a)(2)(ii).

<sup>128</sup> 45 C.F.R. § 164.508 (a)(2)(iii)(iv).

<sup>129</sup> 45 C.F.R. § 164.510 (b).

<sup>130</sup> 45 C.F.R. § 164.510 (c).

<sup>131</sup> 45 C.F.R. § 164.510 (e).

<sup>132</sup> 45 C.F.R. § 164.510 (f).

The HIPPA regulations to not provide private remedies for wrongful disclosure.

### ***K. Regulatory requirements for grantee privacy protection: the animal protection model***

Reforms of federal law to protect data subjects against wrongful disclosure by researchers might follow the model used by Congress to protect animals used as research subjects.

Federal law requires the Secretary of Health and Human Services, acting through the Director of NIH, to require grantees to require research grantees in biomedical and behavioral research to establish “animal care committees” to assure compliance with HHS guidelines.<sup>133</sup> “If the Director of NIH determines that--

“ (1) the conditions of animal care, treatment, or use in an entity which is receiving a grant, contract, or cooperative agreement involving research on animals under this subchapter do not meet applicable guidelines established under subsection (a) of this section;

“ (2) the entity has been notified by the Director of NIH of such determination and has been given a reasonable opportunity to take corrective action; and

“(3) no action has been taken by the entity to correct such conditions;

“[T]he Director of NIH shall suspend or revoke such grant or contract under such conditions as the Director determines appropriate.”<sup>134</sup>

A similar provision could be enacted by the Congress pertaining to the obligation of research grantees to respect data privacy. In the absence of Congressional Action, NIH and other agencies could impose such obligations through rulemaking, drawing implied statutory authority from the Federal Privacy Act.

## **V. Efficacy of Legal Protections**

A number of realities bedevil those who would design systems of legal rights and duties to protect private and commercial interest justifying confidentiality. All of these realities confront advocates of legal protection as a way of enhancing the free flow of confidential information from government sources to private researchers.

The first reality is that, once confidential information is disclosed, it cannot be made confidential again. Once a trade secret becomes public, it no longer is a trade secret. Once someone’s sexual orientation is known, it cannot become secret again.

---

<sup>133</sup> 42 U.S.C. § 289d(b) (2003).

<sup>134</sup> 42 U.S.C. §289d(d).

The second problem is that it is difficult to know if someone half way across the country has disclosed information about oneself or one's commercial activities.

Even if one discovers an impermissible disclosure it is extremely difficult to prove who made the disclosure and even more difficult to prove it in a legal proceeding.

Even when the subject of an impermissible disclosure could in theory prevail in a legal proceeding, in the vast majority of cases the transaction costs of involving the legal system to protect against data disclosure far exceed the damage that can be proven,<sup>135</sup> thus discouraging economically rational individuals and entities from seeking to vindicate their legal rights.<sup>136</sup>

While injunctive relief is available under some legal regimes, injunctions are useful only in that narrow subset of cases in which the data subject discovers imminent disclosure before it occurs, and can get to court fast enough to obtain an injunction to block the disclosure.

## VI. Conclusion

Despite interest in using legal liability to protect data subjects against wrongful disclosure of data about them by researchers receiving data from the federal government, the likelihood of such liability actually being imposed in claims initiated by private persons is low.

If legal liability is to become a realistic protection, government agencies disclosing data to researchers should impose restrictions in licensing agreements, framed so as to support third-party beneficiary suit by data subjects, and should follow the model used to protect animals as research subjects: they should require recipients of sensitive data to have comprehensive internal mechanism to protect the data against improper disclosure, and should cancel contracts and bar future contracts to grantees who fail to comply.

---

<sup>135</sup> Accord, Reidenberg, 54 Hastings L. J. at 896 (noting difficulty of providing monetary damages).

<sup>136</sup> Accord, Reidenberg, 54 Hastings L. J. at 897 (pointing out that cost of litigation discourages individual suits for relatively small provable damages)