AN INFORMATION SOCIETY APPROACH TO PRIVACY LEGISLATION: HOW TO ENHANCE PRIVACY WHILE MAXIMIZING INFORMATION VALUE

DANA BELDIMAN*

INTRODUCTION

As we advance in information society, more and more of the wealth created consists of information. Personal data are an important subset of information and are rapidly becoming a premium commodity. Industry and government collect and use these data for purposes such as marketing, statistics and law enforcement.[1] Many believe that personal information is well on its way to becoming one of the most valuable forms of information in our society.

The advent of the global communications network raises treatment of personal information to a level of acute significance. Technology provides tools that allow processing of unprecedented masses of information; terabytes of digital data can be stored in hundreds of thousands of databases around the world. They can be replicated instantaneously in unlimited numbers and transmitted worldwide at the press of a button. One of the principal areas of concern is that technology has facilitated aggregation of personal data, i.e. data collected by one source for a certain purpose can be combined with data collected by a different source for a different purpose. All of these developments pose a serious risk to personal privacy.[2]

Protection of personal data has emerged as a cutting-edge issue in the new millennium. Most developed countries have passed comprehensive, often quite stringent, legislation to protect privacy of personal data.[3] In the United States, however, no such legislation has been passed. The existing laws are limited to individual sectors of the economy.[4] Consequently, some form of comprehensive legislation in the area of personal information is inevitable.

This paper proposes a combined legal and technological solution to protect privacy in the context of increasing proliferation of personal information. By harnessing the technological capabilities which lie at the root of the problem, greater privacy protection is afforded to the individual, and the value of personal data is maximized for the benefit of both consumer and user.

---

* Dana Beldiman is a partner of the law firm Carroll, Burdick & McDonough in San Francisco. Her practice focuses on intellectual property and electronic commerce law.

[1] Kathleen A. Linert, *Database Marketing and Personal Privacy in the Information Age*, 19 SUFFOLK TRANSNAT'L L. REV. 687, 687-88 (1995) (discussing how easily personal information about spending, marital status, etc. is accessed).

[2] *See id.* (discussing the fact that all personal information is available at the push of a button).

[3] *See id.* at 702-05 (explaining that the European countries have legislation promoting individual privacy by protecting personal data).

[4] *See id.* at 697-98 (qualifying certain legislation as only applicable to the government and not the private sector); *see also infra* text accompanying notes 22-31 (discussing the sectoral nature of U.S. privacy legislation).

OVERVIEW

Part I of this paper discusses the state of privacy legislation in the U.S. and the European Union ("EU"), and the factors that favor passage of personal data privacy legislation in the U.S. These factors are (1) the growing concern about online privacy; (2) the sectoral nature of privacy legislation in the U.S.; and (3) the need for international harmonization of data privacy laws. Part I concludes that for these reasons, legislation in the U.S. is not only necessary but inevitable.

Part II discusses the history and nature of Fair Information Principles ("FIPs") as policy tools underlying privacy legislation, illustrated by means of the Safe Harbor Framework formulation.

Part III examines the structure of personal data transfer transactions. The focus is on how an individual's choices regarding treatment of personal data ("preferences") can be honored in the course of multiple successive ("downstream") transactions. Two elements must be passed on downstream to ensure that preferences are honored: (1) the obligation (whether contractual or imposed by law) to observe the preferences in a manner consistent with the FIPs; and (2) the data themselves, along with information relating to preferences. Part III further discusses possible theories that would support an obligation to honor an individual's privacy preferences. The most appealing model is the law of trade secrets, because it allows the parties the maximum freedom to contract, with only minimal interference by imposed legal norms. Although this model is appealing, the reality remains that the sheer volume of data and preferences makes compliance with the FIPs at an internationally acceptable level extremely burdensome to the data collector or user.

Part IV outlines a concept for a two-prong solution, consisting of a legal and a technological component. The solution addresses the downstream transfer of personal data and preferences by delegating it to a technological infrastructure. Technology is the natural answer to the data problem, because technology lies at the origin of the present proliferation of personal data. The infrastructure ensures that data are permanently associated with their preferences; and that they can be accessed by authorized users. It also performs the requisite FIPs function electronically. Once the data transfer function is outsourced and the FIPs obligation discharged, the legal component falls into place easily. A mandatory norm imposes, by common law or statute, an obligation *erga omnes* to observe the preferences stated by the data subject. This obligation is analogized to the real estate doctrine of a "covenant running with the land," under which a transferee takes property subject to pre-existing obligation incident to the property. The value of data will be maximized, benefiting both data subject and user because the underlying technology allows for a fine-tuning of the data subject's preferences.

I. THE STATE OF PRIVACY LEGISLATION IN THE UNITED STATES AND THE EUROPEAN UNION

A. Factors Favoring Personal Data Legislation

1. Growing Concerns About Online Privacy

Concerns about personal data privacy are on the increase.[5] The use of privacy invasive technologies such as cookies, web bugs, spy ware, etc. is becoming more and more common.[6] Yet the legal basis for finding liability for these invasions is lacking. A case in point is the *DoubleClick* litigation.[7] DoubleClick Inc. collected potentially personally-identifiable information on Internet users, including names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, and web sites visited.[8] The purpose for collecting this information was to build demographic profiles for targeted banner advertisements.[9] The users sued, claiming this information was personal in nature and not what one would ordinarily expect advertisers to be able to collect.[10]

Several actions were filed against DoubleClick, the most notable one being a consolidated class action in the Southern District of New York.[11] The allegations included claims under the Electronic Communications Privacy Act (ECPA), Federal Wiretap Statutes, and the Computer Fraud and Abuse Act (CFAA).[12] In March 2001, the court was forced to dismiss the action, holding that no liability could be established under any of the theories alleged.[13] None of the numerous privacy-related laws were capable of providing redress for DoubleClick's alleged misconduct.[14]

With respect to the ECPA claim, the court found that, because the "electronic information services" were provided through the Internet, DoubleClick was exempt from the ECPA.[15] Accessing cookie identification numbers fell outside the ambit of the statute because the statute only covered "electronic storage" relating to

---

[5] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A FEDERAL TRADE COMMISSION REPORT TO CONGRESS, p. 1, *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (May 22, 2000) [hereinafter FTC, PRIVACY ONLINE].

[6] *Id.*

[7] *In re* DoubleClick Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[8] *Id.* at 502.

[9] *Id.* at 502-03.

[10] *Id.* at 502.

[11] *Id.* at 500.

[12] *Id.* at 499.

[13] *Id.* at 526 (dismissing Plaintiff's federal claims thus vitiating the district court's jurisdiction).

[14] *Id.* (explaining the absence of evidence in legislative and judicial history prohibiting the conduct at issue).

[15] *Id.* at 511.

temporarily stored communications.[16] Although DoubleClick had intercepted electronic communications between plaintiffs and DoubleClick's clients, the wiretap claims were also dismissed because DoubleClick's websites had consented to such interception, and the interception was not done "for purpose of committing a criminal or tortuous act."[17] Finally, the CFAA claims were dismissed because plaintiffs could not establish the damage threshold required for the statute.[18]

Conduct such as that of DoubleClick's is the nightmare of most Internet users.[19] The Federal Trade Commission's ("FTC") Privacy Online Report Survey found that "92% of consumers are concerned (67% are 'very concerned') about the misuse of their personal information online. 76% of the consumers who are not generally concerned about the misuse of their personal information, fear privacy intrusions on the Internet."[20] Yet despite these widespread fears and the outcry of the press when the *DoubleClick* facts first became public, under U.S. law this type of conduct is not actionable.[21]

2. The Sectoral Nature of Privacy Legislation in the U.S.

Unlike other countries, the U.S. has approached personal data legislation by sector.[22] The result is a patchwork of laws that are not particularly compatible. The approach to legislating can best be characterized as "knee-jerk."[23] For instance, disclosure of Supreme Court nominee Robert Bork's video viewing choices in the course of congressional hearings relating to his nomination resulted in prompt passage of the Video Privacy Protection Act.[24]

The most notable examples of sectoral privacy legislation include the Gramm-Leach-Bliley Act ("GLB")[25] the Health Insurance Portability and Accountability Act ("HIPAA"),[26] the Children's Online Privacy Protection Act ("COPPA"),[27] the Privacy Act,[28] the Fair Credit Reporting Act (FCRA),[29] the Electronic Communications

---

[16] *Id.* at 511-12.

[17] *Id.* at 513-18.

[18] *Id.* at 518-26.

[19] *Id.* at 502 (explaining that collected information is considered personal and private).

[20] FTC, PRIVACY ONLINE, *supra* note 5, at 2.

[21] It should be noted, however, that a California state court claim on the same facts settled for an undisclosed amount. Judnick v. DoubleClick, No. CV 000421 (Superior Court, Marin County, Cal. Jan. 27, 2000), http://legal.web.aol.com/decisions/dlpriv/doubleclick.pdf (last visited October 18, 2002). California's state constitution protects consumers from acts invading their privacy. *Id.*

[22] Linert, *supra* note 1, at 698.

[23] *Id.* (stating that U.S. legislation is reactionary).

[24] 18 U.S.C. § 2710 (2000).

[25] 15 U.S.C. §§ 6801-6810 (2000) (regulating disclosure by financial institutions of personally identifiable information).

[26] For legislation governing information collected online, see Act of 1996, Pub. L. No. 104-191, §§ 262, 264; *see also* 45 C.F.R. §§ 160-164.502 (2002) (governing security and privacy).

[27] For legislation governing information collected online from children below the age of thirteen see 15 U.S.C. §§ 6501-6506 (2000); *see also* 16 C.F.R. § 312 (2002).

[28] 5 U.S.C. § 552(a) (2000) (governing the handling of federal employees' personal data).

[29] 15 U.S.C. § 1681 (2000) (governing the handling of consumer credit reports).

Privacy Act (ECPA),[30] and the Video Privacy Protection Act.[31] Altogether, there are more than thirty federal laws, as well as innumerable state laws that affect the handling of personal information.

The existence of so many laws poses problems from both substantive and structural standpoints. Substantively, the numerous discrepant norms that govern personal data, are confusing to consumers and collectors of data alike.[32] From the structural standpoint, each law requires establishment of a particular technological infrastructure. The requirements for the various infrastructures differ because the norms mandating them differ.[33] Absent a common technological standard for collecting, storing and transmitting personal information, the individual regulated sectors will be unable to communicate among themselves.[34] For instance, despite the existence of sophisticated internal storage and processing solutions, information from the healthcare system may have to be transferred manually to that of a bank, because the two architectures are not interoperable. This is a huge cost to society.

Enforcement of data privacy violations falls within the purview of the FTC.[35] The FTC's enforcement authority derives primarily from Section 5 of the Federal Trade Act,[36] which empowers the Commission to "prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce."[37]

Currently, outside the few regulated sectors, such as health and banking, no mandatory norm exists that would impose a particular conduct on collectors of data. Companies are not required to have privacy policies.[38] Enforcement by the FTC is, therefore, limited to violations of a data collector's own voluntarily implemented policy.[39] In other words, a data collector who has no policy at all can engage in the most outrageous privacy transgressions, without falling within the ambit of the FTC. If the data collector is not part of a regulated sector, privacy violations are likely to go unpunished.

Passage of a more comprehensive legislative framework to protect online privacy has been at the center of the public debate for several years. Numerous bills were introduced into Congress in 2000 and early 2001, and passage of a law was expected imminently. However, in early October 2001, a sudden shift of direction occurred when the Chairman of the FTC announced an agenda focused on tougher

---

[30] 18 U.S.C. § 2701 (2000) (containing provisions regarding the interception of wire, oral and electronic communications, and the unauthorized access to stored data).

[31] *Id.* at § 2710 (prohibiting wrongful disclosure of video rental records).

[32] Maj. R. Ken Pippin, *Consumer Privacy on the Internet: It's "Surfer Beware"*, 47 A.F. L. REV. 125, 140 (1999) (explaining that most internet users are not experienced users).

[33] Suzanne M. Thompson, *The Digital Explosion Comes With a Cost: The Loss of Privacy*, 4 J. TECH. L. & POL'Y 3, 26 (1999) (discussing industry norms which provide standards for control).

[34] *Id.* (stating that legal regulation usually protects a single activity or area and does not address all issues of collections, storage, use, and disclosure).

[35] Pippin, *supra* note 32, at 133 (discussing how the FTC enforces consumer protection laws).

[36] 15 U.S.C. §§ 41-58 (2000).

[37] *Id.*

[38] *See* FTC, PRIVACY ONLINE, *supra* note 5, at 34. In its Privacy Online Report, the FTC makes recommendations as to norms that should govern online data collection activities. These norms follow the generally accepted fair information practices of Notice, Choice, Access and Security, but remain purely voluntary. *Id.* at 36-37.

[39] *Id.* at 33-34.

enforcement of existing laws, rather than passage of new legislation.[40] In his speech Chairman Muris stated "there is a great deal we can do under existing laws to protect consumer privacy. . . . We will use our full arsenal of tools – cases, changes to our Telemarketing Sales Rule, workshops, and education. . . ."[41] Unfortunately, this "arsenal" sounds less than impressive, and the absence of adequate "weapons" can lead to aberrations. Most notably, the FTC announced in early 2002 that it will hold companies' offline activities to the promises made with respect to their online activities.[42]

3. The Need For International Harmonization

In a global economy, it is virtually impossible to confine personal data to national borders. Multinational companies, financial institutions, airlines, and credit card companies cannot function without transferring data between countries.[43] The absence of a harmonized legal system impedes the trans-border flow of data.[44]

Under the laws of most European countries, protection of personal data is a fundamental human right.[45] Europeans are very concerned that transmitting sensitive data to a country with different privacy standards will lead to their unauthorized proliferation, particularly via electronic means.[46]

Most of the current European Union ("EU") member states' data protection laws derive from the European Union Data Protection Directive ("Directive").[47] The Directive contains fundamental principles pertaining to data protection and has been adopted in almost all member states.[48] The Directive requires national laws to set stringent standards for protection of the information collected about an identified or identifiable individual, whether or not the data is publicly available.[49] The Directive

---

[40] Timothy J. Muris, FTC Chairman, Remarks at the Privacy 2001 Conference, Cleveland, Ohio, (October 4, 2001), *at* http://www.ftc.gov/speeches/muris/privisp1002.htm.

[41] *Id.*

[42] J. Howard Beales III, Director of FTC Bureau of Consumer Protection, at the Annual Meeting of Promotion Marketing Association, December 5, 2001, *at* http://www.ftc.gov/speeches/other/bealesconsumprotectagenda.htm.

[43] For an overview of the kinds of personal information involved in transborder exchanges, see REINHARD ELLGER, DER DATENSCHUTZ IM GRENZUBERSCHREITENDEN DATENVERKEHR 108-29 (1990). Ellger finds that the most intensive transborder data flows occur in the following areas: (1) personnel departments; (2) banks, insurance companies, credit card companies, and credit bureaus; (3) direct marketing; (4) airlines, travel agencies, and other business involved in tourism; (5) companies that seek to deliver goods to or otherwise trade with international customers; and (6) within the public sector: police, customs, tax departments, and public pension agencies. *Id.*

[44] Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace,* 52 STAN. L. REV. 1315, 1351 (2000).

[45] *Id.* at 1347.

[46] *Id.* at 1351.

[47] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data,* 1995 O.J. (L 281) 31 [hereinafter *Directive 95/46/EC*]. This directive is scheduled for implementation in all member states, however, the process of implementation is still ongoing as of the date of this writing. *Id.*

[48] For instance, in May 2001, Germany revised its data protection law to effectively incorporate the provisions of the Directive. *Id.*

[49] *Id.*

further requires an individual's consent prior to processing personal information for purposes other than those contemplated by the original data collector.[50] Member States may restrict the processing of defined "sensitive" data such as religious or sexual preferences and health information.[51] Collection and use of personal information not relevant for the stated purpose of processing is restricted.[52] The Directive further imposes rules of transparency, notice to data subjects, access of data subjects to their data and the ability to correct any errors.[53] Organizations must maintain appropriate security for the processing of personal information. [54]

To avoid circumvention of the stringent European laws by transfer outside the EU, the Directive includes provisions that ensure that European rules govern all personal information.[55] The trans-border data flow provision prohibits the transfer of personal information to countries that do not have "adequate" privacy protection.[56] The "adequacy" requirement can be met by either: (1) a finding of the European Commission that a third country ensures an adequate level of protection;[57] or (2) via contractual obligations between the parties exchanging data.[58]

Contractual obligations can be set forth in an agreement between the parties exchanging data.[59] The agreement must require the non-EU importer to follow the data protection law of the member state in which the data exporter is located.[60] Alternatively, model clauses prescribed by the EU Commission can be used. These clauses are valid for all EU member countries and avoid the inconvenience of multiple legal regimes.[61]

Because the privacy legislation prescribed by the EU is so comprehensive and touches upon all spheres of the economy, many businesses view it as being too onerous.[62] Groups in the EU member states have advocated simplification of what was perceived as over-regulation. Nonetheless, other countries are looking at the European Directive as the basic model for information privacy. Canada, as well as countries in South America and Eastern Europe are adopting EU-style privacy

---

[50] *Id.* at arts. 14, 15.

[51] *Id.* at art. 8, ¶ 4.

[52] *Id.* at art. 6.

[53] *Id.* at arts. 9-12, 14-15, 18-19, 21.

[54] *Id.* at art. 17.

[55] *Id.*

[56] *Id.* at art. 25.

[57] *Id.* The European Commission has found that some countries, for example Switzerland and Hungary, provide "an adequate level of protection." *Id.*

[58] *Id.* at art. 26, cl. 2.

[59] *Id.* at art. 26.

[60] *Id.*

[61] The model contractual clauses consist of ten clauses and several appendices and generally cover the following areas: (1) obligations of the data exporter; (2) obligations of the data importer; (3) liability; (4) applicable law and enforceability of the clauses; and (5) jurisdiction. The model clauses have received considerable criticism from business groups, based on the fact that they are unnecessarily burdensome and prescriptive, that they impose joint and several liability on the data importer and exporter, and that they require the data importer to submit to the jurisdiction of the member state from which the data originated.

[62] Jane Black, *Self-Policing on Privacy? Forget It*, BUSINESS WEEK (July 6, 2001), *available at* http://www.businessweek.com/bwdaily/dnflash/jul2001/nf2001076_893.htm.

laws.[63] One of the perceived reasons for doing so is "the conceptual appeal of a comprehensive set of data protection standards in an increasingly interconnected environment of online and offline data."[64]

The European Commission considered U.S. privacy laws and concluded that the protection offered by the U.S. laws is not "adequate" protection for purposes of data transfer from the EU to the U.S. This fact imposes a considerable burden on cross-border business between the U.S. and EU member states. To resolve this potential clash, the U.S. and EU negotiated the "Safe Harbor Framework," which would allow individual companies to implement procedures deemed "adequate" for receipt of data from the EU.[65]

The Safe Harbor Framework consists of a set of principles that establish procedures relating to transfer of personal data. U.S. data recipients who adhere to the principles set forth by the Framework will be deemed to provide an adequate level of protection.[66] The Safe Harbor principles reflect the U.S. approach to privacy but at the same time are designed to meet the European Union Privacy Directive requirements.

Although the Safe Harbor framework has been adopted, it does not resolve the fundamental differences between the two systems.[67] Because it is cumbersome to implement, the program has been slow to start.[68] In the two years since its adoption, less than 200 U.S. companies have joined the Framework, and few of them are Fortune 500 companies.[69] Companies complain that adhering to the Framework subjects them to enforcement by both the EU and the FTC. The Safe Harbor has also been criticized because it gives preferential treatment to personal data of non-U.S. nationals, while personal data of U.S. citizens are subject to U.S. law that even in legislated sectors in the U.S. is less stringent.[70]

The three factors discussed above – the growing concerns about online privacy, the sectoral nature of U.S. privacy legislation and the need for international harmonization -militate strongly for adoption of privacy legislation. The question is not so much whether regulation of personal data will be passed in the U.S., but what norms this type of law should contain to accomplish the desired policy goals. The following section will examine the Fair Information Principles, the leading policy

---

[63] Joel R. Reidenberg, *E-Commerce and Privacy Institute for Intellectual Property and Information Law Symposium: E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 737 (2001).

[64] *Id.*

[65] U.S. DEP'T OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (July 21, 2000), http://www.export.gov/safeharbor/SHPRINCIPLESFINAL [hereinafter SAFE HARBOR].

[66] U.S. Dep't of Commerce, Cover letter from Robert S. LaRussa, Acting Under Secretary for International Trade Administration, to U.S. organizations (July 21, 2000), http://www.export.gov/safeharbor/sh_documents.html.

[67] *See generally* Lynn Chuang Kramer, *Comment, Private Eyes Are Watching You: Consumer Online Privacy Protection –Lessons from Home and Abroad*, 37 TEX. INT'L L.J. 387, 396-411 (2002) (comparing the EU and U.S. systems).

[68] Reidenberg, *supra* note 63, at 746 (noting that after 7 months of the Safe Harbor Framework coming into effect, fewer than fifty-five organizations were participating); *see also* Kramer, *supra* note 67, at 399 (noting that after 1 year, less than 135 companies were participating).

[69] U.S. DEP'T OF COMMERCE, SAFE HARBOR LIST (2002), *available at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (listing organizations that self-certify to adhere to the Safe Harbor Framework).

[70] Reidenberg, *supra* note 63, at 746.

tools for privacy regulation. These principles are recognized by the EU Directive, the Safe Harbor Principles and existing U.S legislation and constitute a *sine qua non* element of legislation in the field of privacy.

II. HISTORY AND NATURE OF FAIR INFORMATION PRINCIPLES

A. Fair Information Principles as Tools for Privacy Regulation

Fair Information Principles ("FIPs") are norms for the treatment of personal data shared across cultures. They are the leading policy tool for privacy regulation in the U.S. and elsewhere and have been incorporated into most privacy laws.[71] The U.S. began developing these principles in the 1970's.[72] Their present form appeared in the 1980's in such privacy legislation as the Privacy Act and the Fair Credit Reporting Act.[73] They also are present in early European privacy provisions, such as the OECD guidelines.[74]

The FIPs have been formulated in different manners, but apart from minor variations, the core principles are the same.[75] At a fairly high level of abstraction, Paul Schwartz, one of the leading authors on privacy issues, articulates four FIPs as follows: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external or governmental oversight.[76]

One of the earliest expressions of the FIPs in U.S. legislation is contained in the Privacy Act of 1974. The Act provides that: (1) there should be no secret record keeping systems; (2) information collected for one purpose should not be used for another purpose without the consent of the individual; (3) individuals should be given access to information held about them and the opportunity to correct or amend that information; (4) information is kept relevant, accurate and up to date; and (5) information is protected against unauthorized loss, alteration and disclosure.[77] The substance of these principles has been incorporated to varying degrees in subsequent legislation.

---

[71] FTC, PRIVACY ONLINE, *supra* note 5, at 3.

[72] In 1974 Congress passed the Privacy Act. However, this statute only protected personal information held by the federal government. A REVIEW OF THE FAIR INFORMATION PRINCIPLES: THE FOUNDATION OF PRIVACY PUBLIC POLICY, *at* http://www.privacyrights.org/ar/fairinfo.htm (last visited Oct. 12, 2002).

[73] 15 U.S.C. § 1681 (1994).

[74] Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, O.E.C.D Doc. C (80) 58 (Final), adopted Sept. 23 1980.

[75] Reidenberg, *supra* note 44, at 1325.

[76] Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information,* 76 TEX. L. REV. 1 (1997) [hereinafter Schwartz, *Health Care Information*]; *see also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999) [hereinafter Schwartz, *Privacy and Democracy*].

[77] M. ROTENBERG, THE PRIVACY LAW SOURCEBOOK 2002, ELECTRONIC PRIVACY INFORMATION CENTER, p. 39.

The Safe Harbor Framework[78] lists seven principles that are consistent with both formulations mentioned above. Its first four principles (notice, choice, access and security) are also contained in the FTC's Privacy Online Report.[79] Because the Safe Harbor formulation meets the requirements of both the EU and the U.S., and because it is stated in a comprehensive, succinct and specific manner, it will serve as analytical framework for this paper. Furthermore, the fact that these principles have been agreed upon by the both EU and the U.S. in the course of the Safe Harbor negotiations supports the notion that they enjoy wide acceptance.[80]

The following will summarize the requirements of the Safe Harbor FIPs:

NOTICE: Organizations must notify data subjects that information is being collected, for what purpose it is collected, how individuals can contact the organizations with inquiries and complaints, to whom information is disclosed, and what choices the individual has for limiting use and disclosure.[81]

CHOICE: "Organizations must give individuals the opportunity to choose ("opt out") whether their personal information [may be] disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit ("opt in"), choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual."[82]

ONWARD TRANSFER: "Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the directive [or a finding of "adequacy"]. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles."[83]

ACCESS: Generally, "individuals must be given access to personal information about them that an organization holds." They must "be able to correct, amend, or delete that information where it is inaccurate." Exceptions to this general rule are permitted "where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated."[84]

SECURITY: "Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction."[85]

DATA INTEGRITY: "Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current."[86]

---

[78] SAFE HARBOR, *supra* note 65, at http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.

[79] FTC, PRIVACY ONLINE, *supra* note 5, at iii.

[80] SAFE HARBOR, *supra* note 65, at http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *Id.*

ENFORCEMENT: An organization must have "readily available and affordable independent recourse mechanisms [that allow] each individual's [complaints] to be investigated and resolved and damages to be awarded where the applicable law or private sector initiatives so provide." In addition, the organization must establish procedures for verifying that the commitments to adhere to the Safe Harbor Principles are implemented. Finally, the organization must remedy problems arising out of a failure to comply with the principles. "Sanctions must be sufficiently rigorous to ensure compliance by the organization."[87]

An additional principle that is not mentioned in the Safe Harbor Framework is the principle of FINALITY, which prohibits an organization from processing personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual.[88] It is one of the main principles of the European Directive, and it has been recognized in the U.S. in legislation such as the Privacy Act and in case law arising under it. [89]

III. STRUCTURE OF PERSONAL DATE TRANSER TRANSACTIONS

A. Protection Of Personal Data In Downstream Transactions (Onward Transfer)

Personal data differ from other types of intellectual property in the nature of their use. While patents and copyrights are typically subject to a single transfer, from the inventor or creator to the user,[90] personal information is, as a rule, subject to numerous successive transfers.[91] This is due to the fact that, unlike other intellectual property, the value of personal data lies in their ability to be re-used multiple times, rather than in their intrinsic value, which often is minimal.[92] Frequent re-use brings with it the risk of frequent invasions of privacy, as the following scenario illustrates.

Assume an individual makes a purchase from Amazon.com. She discloses personal information in reliance on Amazon's stated privacy policies. The policies

---

[87] *Id.*

[88] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, STAN. TECH. L. REV. 1, 31 (2001).

[89] Britt v. Naval Investigative Serv., 886 F.2d 544, 549 (3d Cir. 1989) ("Congress limited interagency disclosures to more restrictive circumstances. There must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."); *see also* Covert v. Harrington, 876 F.2d 751, 755 (9th Cir. 1989) (stating that information collected for security clearance purposes is incompatible with disclosure for criminal investigation of subsequent actions); Mazaleski v. Treusdell, 562 F.2d 701, 713 n. 31 (D.C. Cir. 1977) (finding that derogatory information concerning a federal employee's dismissal not compatible with disclosure to prospective employer).

[90] Even in a situation involving multiple licensees, the transaction is ordinarily between owner/inventor and licensee, as opposed to from one licensee to another. The value to the user lies in the substance of the property, and not, as with personal information in the ability to transfer it.

[91] Anna E. Shimanek, *Do You Want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles*, 26 IOWA J. CORP. L. 455, 457-68 (2001).

[92] *Id.* at 457.

provide that the information will not be used for solicitation and will not be sold to third party marketers or aggregators. Amazon abides by these policies. However, Amazon then sends the purchase out for fulfillment to FedEx, along with the individual's personal information. FedEx has a different policy and promptly turns around and sells the data to an aggregator, such as Acxiom.[93] The aggregator may already have a file on the particular individual, a file which contains information derived from sources such as a local grocery store or the DMV. Even though some of the data may be anonymous, in many cases, they contain enough clues to be matched with an already existing file. These aggregated data are then sold or leased many times to advertisers in the direct marketing industry.

This scenario shows that even though the data subject's instructions on the handling of there data were observed in the first transaction, the data subject's privacy was breached because her instructions were not communicated and not observed in subsequent transactions. This scenario can be avoided by implementing the concept of "onward transfer." This concept essentially limits transfer of data to third parties who do not have adequate data protection measures in place. Under the Safe Harbor formulation of this principle, the collector of personal data may transfer information to a third party only if the third party (1) subscribes to the Principles; (2) is subject to the Directive or other adequacy finding; or (3) enters into a written agreement to provide at least the same level of privacy protection as is required by the relevant Principles.[94] This essentially means that a transferee of data must either be governed by a law which protects data in accordance with specified Principles, or must contractually agree that it will do so; otherwise the protection of the personal data transferred is not ensured.

Yet "onward transfer" has received little in-depth treatment from commentators and courts. The concept is present to a very limited extent in U.S. legislation and only on a sectoral basis[95] and it is conspicuously absent from the FTC Report formulation. Nonetheless, this principle is key in structuring norms of conduct governing personal data privacy, because a law that fails to protect privacy in the course of downstream transactions offers only illusory protection.

---

[93] Acxiom maintains the largest collection of personal data outside the U.S. Government. Its database contains detailed information about 160 million people and its contents is made available to the marketing industry via services such as "[a]cquire new numbers for telemarketing," "[a]ppend telephone number to name and address," or "[l]inkage to individual customer information from multiple data sources for specific marketing applications." ACXIOM, CORPORATE OVERVIEW, *at* http://www.acxiom.com/DisplayMain/0,1494,USA~en~514~3100~0~,00.html (last visited Oct. 11, 2002).

[94] *See* SAFE HARBOR, *supra* note 65, at http://www.export.gov/safeharbor/SHPRINCIPLESFINAL ("Where an organization wishes to transfer information to a third party that is acting as an agent, . . . it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.")

[95] For example, regulations under the Gramm-Leach-Bliley Act require financial institutions to enter contractual agreements with service providers to whom non-public personal data are disclosed, prohibiting further disclosure and use of the data for purposes other than for which they were disclosed. 12 C.F.R. § 216.12 (2000). Additionally, the HIPAA Standards for Privacy of Individually Identifiable Health Information provides for "de-identification" of personal information by removing individually identifiable information. De-identified information may be used or disclosed freely as long as no means of re-identification is disclosed. 45 C.F.R. § 165.514 (2000).

B. The Anatomy of Downstream Transactions

Before considering norms of conduct governing downstream transfer, it is helpful to analyze the mechanism of downstream data transactions.

> Assume A, an individual (referred to as "data subject"[96] in this paper) enters into a transaction with B, a data collector or user, in which A allows B to use A's data in exchange for consideration. The transaction between A and B works in practice, because A has data that are of value to B and the power to exclude B from access to the data. Because the data are valuable to B, B is willing to pay for access and also to make a promise that the data will be treated in accordance with A's preferences. If B breaches, A can sue for damages. Up to this point, the marketplace has achieved a workable outcome.

If the data are to be transferred downstream in a subsequent transaction from B to C and from C to D, the marketplace model does not necessarily hold true. To protect A's interests, the downstream transaction must consist of the following bargain: B provides the data to C in exchange for payment, accompanied by two promises: (1) that C will honor A's preferences and otherwise abide by the FIPs[97] and (2) that C will elicit the same promises (i.e. to observe A's preferences and to elicit a promise to the same effect from its transferee) from D. Although A is now out of the picture as far as the transaction is concerned, A's preferences still govern the use of the data. In effect, B, C and any other downstream sellers act as agents for A, in that they protect A's preferences. Two difficulties arise: (1) the transaction costs are increased by eliciting the additional promises from the downstream transferee;[98] and

---

[96] The term "data subject" is borrowed from the European Directive and the Safe Harbor Principles, and refers to the individual whose personal data are at issue.

[97] *See* Jeffrey B. Ritter et al., *Emerging Trends in International Privacy Law*, 15 EMORY INT'L L. REV. 87, 131-32 (2001). If A's interests are to be fully protected, B would be responsible for the following:

> The effective delivery of notice to the data subject in connection with the original collection of the personal data; the adequacy of that notice under any applicable legal requirements that regulate the collection; the proper recognition (and disposition) of any opt-in/opt-out elections by the data subject, and the adequacy of the records relating to such elections; the accuracy and integrity of all records created in which the personal data has been collected and maintained; the consistency of usage of the data - i.e., the collector and any processor (including A) have used the data consistently with the disclosures made in the notice provided to the data subject; and the maintenance of suitable access and correction processes relating to inaccurate information (necessary to assuring B of no secondary liability for processing or relying upon inaccurate information).

Id. The requirement of abiding by the FIPs imposes a huge additional burden on the transferee. One could argue that this burden is not required by A. However, the fact is that by the time the data have undergone dozens of transfers A will have lost track of them, and can only be protected by the practices incorporated by the FIPs.

[98] An additional component to be considered is the cost of honoring A's preferences. This may exceed the transaction costs, because it requires the establishment and maintenance of a complex infrastructure and reduces the consideration received by the transferor. Alternatively, this cost

(2) consideration for the promises reduces the payment to the transferor. This is troublesome because the beneficiary of the promises is A and not the transferor. Otherwise viewed, B, C, D and others act as agents for A without being paid by A. This does not make for a sustainable model without further norms being imposed by common law or statute.

To summarize, a comprehensive and viable solution must find a way to include in each downstream transfer of data (1) the obligation to comply with the data subject's preferences and abide by the FIPs and (2) the preferences themselves. The following section will discuss potential legal bases for the obligation to comply with the data subject's preferences.

C. Legal Bases for Norms Protecting Personal Data Privacy

The concept of protecting personal data privacy is not new to U.S. law. Review of the sectoral legislation governing privacy of personal data indicates clearly that an individual's privacy as it relates to personal information deserves some level of protection.[99] Conceptually this protection could derive from a number of possible sources such as a property right,[100] similar to the one that exists in other types of intellectual property, or the "penumbrae" of tort rights protecting against invasion of privacy.[101] Alternatively, it could be based on an unjust enrichment theory[102] or arise out of the legislature's concern about individuals' cognitive difficulties in appreciating the risks of supplying personal data to the private sector.[103]

Different legal theories have been proposed as solutions for the data privacy issue. One suggested approach is to grant individuals a property right in their personal information.[104] The transfer of personal information would occur based on the same rules as the transfer of tangible property and would be governed by market mechanisms. Depending on the individual's perception of the value of her personal information, a price tag would be associated with the transaction.[105] This method is perceived as a simple way to convey the individual's preferences to the market and it

---

could be viewed as a business risk to the data collector. After all, if the cost of doing business exceeds the revenue, maybe data collection is not a viable business. *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1298 (2000).

[99] *See* HIPAA standards, 45 C.F.R. § 165.514 (2000); The Gramm-Leach-Bliley Act Regulations, 12 C.F.R. § 216.12 (2000); The Privacy Act, 5 U.S.C. § 552a (2000).

[100] *E.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYPERSPACE, at 160-61.

[101] Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV 743, 777-78 (2000).

[102] The argument has been made that failure to control the use of personal information, would allow a sort of free riding, or unjust enrichment without compensating the people whose existence makes the enrichment possible. A telling example is that in 1988, the three leading credit bureaus made almost $1 billion from selling credit information, while paying the consumers whose information they were selling zero. E. Volokh, *Free Speech and Information Privacy*, 52 STAN. L. REV. 1049, 1074 (2000).

[103] Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV.1125, 1144 (2000).

[104] LESSIG, *supra* note 100, at 160-61.

[105] Paul M. Schwartz & Joel R. Reidenberg, *BOOK REVIEW: A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CALIF. L. REV. 751, 767-68 (1999).

presents the advantage of not requiring legislative or judicial intervention in the normal course of the transactions.[106]

Others have rejected the property model for such reasons as the market failure for personal information,[107] concerns about incoherence in the field of intellectual property law if personal information receives the same treatment as other categories of intellectual property,[108] or the view that information privacy may be a fundamental civil right, one that cannot be left to the vagaries of the market.[109]

A further reason for rejecting a property model relates to the genesis and function of personal information. Intangible assets - patents, trademarks or copyrights - are created by individuals and granted protection by society for policy reasons.[110] Personal information is created by society at large to fulfill a very specific function, viz. identification of individuals.[111] An individual's exercise of the right to exclude others from using her personal information could interfere with essential public needs. Consider the difficulty of identifying "the Artist Formerly Known As Prince." If individuals had the right to withdraw not just their names, but their social security numbers, addresses, educational information, health records, etc. from public use, chaos would be inevitable.[112] Finally, concerns have also been expressed that the property model could give rise to tensions with the First Amendment.[113]

The scholarly debate has also considered liability models.[114] The criticisms of these models include the facts that: (1) a post-disclosure remedy in the form of damages does not adequately compensate the data subject; and (2) a liability model alone does not provide for a mechanism to control how the data are treated downstream.[115]

Review of these authorities makes it evident that the exact nature of the doctrine protecting personal data is still subject to debate, as is the extent and form of an individual's right in personal data.[116] Nonetheless, the principle that can be distilled from existing legislation and case law is that individuals have, at a minimum, some right to control the use of their personal information as it relates to

---

[106] *See* Carl Shapiro & Hal R. Varian, *U.S. Government Information Policy* (July 30, 1997) *at* http://www.sims.berkeley.edu/~hal/Papers/policy/policy.html (last visited Oct. 12, 2002); *see also* Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM (Sept. 1996).

[107] Schwartz, *Health Care Information, supra* note 76, at 31.

[108] Schwartz & Reidenberg, *supra* note 105, at 776.

[109] Samuelson, *supra* note 103, at 1142. The option of granting an individual rights in their personal property based on a moral rights theory has also been considered and rejected. *Id.*

[110] *E.g.*, U.S. CONST. art. I, § 8, cl. 8. The policy underlying patents and copyrights encourages Congress to "promote the progress of science and useful arts by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." *Id.*

[111] In addition to the basic "identification" function, personal data serve an "evaluation" function, i.e. by placing an individual's personal information into context in the public forum, society is able to make political decisions. Schwartz, *supra* note 101, at 760.

[112] Concerns about withdrawal from public use of terms necessary to identify common objects also lies at the basis of the bar for registration of generic trademarks. *See* CES Publ'g Corp. v. St. Regis Publ'ns Inc., 531 F.2d 11 (2d Cir. 1975).

[113] *See* Volokh, *supra* note 102, at 1088. However, the First Amendment covers "information." If a norm limiting disclosure applies only to "data," the First Amendment is probably not violated.

[114] *See* S. Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6 (2000).

[115] *See* Samuelson, *supra* note 103, at 1132.

[116] *See* Mark A. Lemley, *Private Property*, 52 STAN. L. REV. 1545, 1545-46 (2000).

protection of their privacy.[117] This standard will be used as premise for the discussion that follows.

D. The Law of Trade Secrets – a Viable Practical Model?

The focus of the present paper is to find a practical solution that would protect personal data privacy in downstream transactions. An appealing model, which combines both property and liability concepts, is the law of trade secrets.[118] The mechanism of transacting personal data transfers could easily follow that of a trade secret transfer; both types of transactions are based on a contract, wherein the consideration consists of a monetary or other *quid pro quo* accompanied by a promise. The promise in trade secrets transactions is confidentiality, while in personal information transactions the promise would be to observe the data subject's preferences and the FIPs and to pass on the obligation to subsequent transferees.

From a policy standpoint, trade secret law is premised on a societal interest in stimulating invention and prohibiting immoral commercial conduct.[119] To achieve this, the law has recognized a quasi-property right in the owner of the trade secret.[120] The law further provides that information designated by its owner as a trade secret may not be disclosed to third parties.[121] The law does not further concern itself with the terms of the contract, the type of property, its value, commercial terms, etc. These are left up to the parties. General liability concepts are used to impose a limited number of default terms. This model is appealing because it allows the parties maximum bargaining power in conjunction with a minimum number of legislated norms[122] while adequately protecting the trade secret owner's interests in the event of a breach.

---

[117] *See supra* text accompanying notes 101-03.

[118] Samuelson, *supra* note 103, at 1152.

[119] Based on the public policy that proscribes immoral commercial conduct, trade secret law contains a minimal number of default terms and procedural provisions. Trade secret law also provides a right against third party users of protected information. A third party which knows or has reason to know that the information has been obtained by improper means incurs liability. If the third party obtained the information innocently, unauthorized use may be prevented after notice to the innocent user. *See generally* California Uniform Trade Secrets Act, CAL. CIV. CODE § 3426 (2002).

[120] Ruckelshaus v. Monsanto, 467 U.S. 986, 987 (1984).

[121] "One is subject to liability for the appropriation of another's trade secret if . . . (b) the actor . . . discloses the other's trade secret . . . and, at the time of the . . . disclosure, (3) the actor knows or should know that the information is a trade secret that the actor acquired from or through a person who acquired it by means that are improper . . . or whose disclosure of the trade secret . . . constituted a breach of a duty of confidence owed to . . . the other." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995).

[122] A look at the provisions of the Uniform Trade Secrets Act confirms the simplicity of the legislative scheme, premised on the public policy against immoral commercial conduct. The main operative provisions are contained in Sections 1-3. Section 1 entitled "Definitions" defines not only the property to be protected, but also the conduct proscribed. Trade secrets are defined as having independent economic value and as being subject to efforts to keep them secret. The prohibited conduct is defined in paragraph (2) of Section 1. Sections 2 and 3 provide for injunctive relief and damages. 18 U.S.C. § 1905 (2002).

A similar structure could work for the transfer of personal information. The policy underpinning of personal data protection is the societal interest in protecting individual privacy. This would be implemented by recognizing a quasi property interest in the individual's personal data, expressed as an individual's right to control the use of personal data under certain circumstances. [123]

Similar to trade secrets, a mandatory norm[124] would further provide that personal data cannot be disclosed or used, except in the manner provided by the owner. This type of structure would allow the data subjects to contract freely for the transfer of personal data, with the assurance that they would be treated in accordance with their preferences.[125]

The comparison works well for transactions between A and B and possibly B and C, but thereafter breaks down. Because in trade secrets successive transfers are the exception rather than the norm,[126] trade secret law does not offer a true solution for the downstream transfer of obligations. Otherwise stated, in the transaction between A and B, B is legally obligated to observe A's preferences. When B transfers the data to C, A may have a contract-based remedy against B, but A will have no basis for preventing C, D and subsequent transferees from misusing the data, because no privity of contract exists. To adequately compensate A, B would have to be held responsible for all subsequent possible misuses of the data. It is in the nature of their use that personal data are transferred countless times to successive transferees. If B were to be held responsible for possible misuse by each of these countless transferees, B's liability would be proportionate not to his own misconduct, but to an unpredictable number of successive transferees.

Several solutions could be adopted as a "fix" to this inequitable result. One possibility would be to designate A as a third-party beneficiary to the agreement between B and C, and also in subsequent transactions. This would permit A to enforce the promise to observe preferences against downstream transferees. If one of them failed to designate A as a beneficiary, A could have a remedy against that particular transferee.

Alternatively, the indemnity model has been suggested for downstream transfer of obligations and shifting the risk of non-compliant conduct.[127] This model avoids judicial intervention by expressing an obligation in contractual terms, whereby one party agrees that in specified circumstances, including its own wrongdoing, it will compensate the other party. This process is flexible, because it allows the parties to negotiate indemnity for certain perceived risks that may not necessarily be cognizable as wrongdoings under the law.[128] In practice it would work as follows: in the event onward transferees fail to respect the terms under which the data were

---

[123] These principles are already present in U.S. law. *See supra* note 95 and text accompanying notes 101-03.

[124] *See* Schwartz, *Health Care Information, supra* note 76, at 51-75 (explaining that mandatory rules are preset expressions of policy choices made by the legislature, which cannot be waived or negotiated around).

[125] *Id.* at 60-61.

[126] *See supra* text accompanying notes 90-91.

[127] Ritter, *supra* note 97, at 131-32 (requiring A to indemnify B for any damages resulting from A's delivering of bad data to B). Indemnification assures the transferor that damages resulting from non-compliant conduct shift to the transferee along with the data. *Id.* at 132.

[128] *Id.* at 127.

originally transferred from A to B, B will be liable to A. To protect itself against this liability, B will ask C to assume responsibility for its own conduct and for that of onward transferees, and C will ask D and so on. Purely contractual indemnity is a viable model only if the transferee has the financial resources to satisfy the indemnity agreement. Because A has no control in selecting the transferee and consequently cannot assess his financial strength, this is an unfair risk to impose upon A.[129]

Finally, the obligation could be passed on downstream via a duty implied by law. This concept is slightly different, in that it is imposed by law rather than negotiated by the parties.[130] The mechanism however, is not foreign to U.S. courts.[131] For instance, California law implies a covenant of good faith and fair dealing into every contract.[132] In the same manner, an obligation to honor preferences could be implied into every data transfer contract, regardless of whether the data are transferred by the data subject or a subsequent recipient. This would relieve A and each successive transferee of the burden of bargaining for the promise and of the risk of diminishing their *quid pro quo*.

All of these doctrines present a certain theoretical appeal. However, in practice they give rise to problems for both the data subject and the collector or user.

From the data subject's point of view, a contract-based solution is unsatisfactory because not all data are captured in settings which allow the data subject to state its preferences. For instance, data that are derived from sources such as public or government databases would not be subject to contractual obligations imposed in an *inter partes* transaction. Coverage of these data can only be ensured by a norm imposed *erga omnes* via common or statutory law.

From the collector or user's point of view, compliance with the requirements of the Fair Information Principles can be very onerous.[133] Providing notice by mail every time an individual's data are used or transferred would involve a prohibitive cost to the user and deluge the data subject in a flood of unwanted paperwork. Similarly, each user would have to put in place a technological infrastructure which allows for the segregation of data, depending on the opt in or opt out choices made by the data subject, and ensures that the data subject has the ability to access and correct the data maintained by the user. This infrastructure would have to be interoperable, at least to some extent with other similar infrastructures, in order to allow for the transfer of data along with the associated preferences. The solutions discussed do not address these problems.

---

[129] *Id* at 131.

[130] RESTATEMENT (SECOND) OF CONTRACTS § 4 (1981) (discussing contractual obligations implied at law). The Restatement (Second) states:

> unlike true contracts, quasi-contracts are not based on the apparent intention of the parties to undertake the performances in question, nor are they promises. They are obligations created by law for reasons of justice. Such obligations were ordinarily enforced at common law in the same form of action (assumpsit) that was appropriate to true contracts.

Id.

[131] *Id.*

[132] Seamen's Direct Buying Serv. v. Standard Oil, 129 Cal. App. 3d 416, 181 Cal. Rptr. 126 (1982).

[133] Schwartz, *Health Care Information*, *supra* note 76; *see also* Schwartz, *Privacy and Democracy in Cyberspace*, *supra* note 76.

Finally, the above legal solutions leave the transfer of the data and preferences to the parties. Apart from being cumbersome to the collector or user, this method does not afford particularly good protection to the data subject. The data are normally subject to hundreds or even thousands of downstream transactions, many of which involve human intervention and consequently a increased risk of error. In the course of these multiple successive transfers, the data may easily become lost, corrupted or disassociated from their preferences and no resource exists to verify their accuracy.

IV. A TWO-PRONGED SOLUTION: LAW AND TECHNOLOGY COMBINED

To find an answer to these questions, it helps to take a step back and consider the origin of the data protection problem. Clearly, the present predicament arises out of an unprecedented proliferation of large quantities of data resulting from rapid technological development. Modern information technology has created capabilities for collecting, storing, retrieving and transferring data that have never existed in the past. Because these capabilities lie at the root of the current proliferation of data, these same capabilities must be looked to in seeking a solution to the data privacy problem. This paper proposes an integrated law-technology solution, whose advantages are obvious.

First, a technology-based solution would reduce the cost of compliance to data users. The cost of manually or semi-manually performing the functions of notice, choice, access, data integrity and onward transfer under a comprehensive data privacy regulation would be prohibitive. An electronic infrastructure designed for this purpose could reduce the cost of these transactions to a minimum.

Second, a technology-based solution enhances the utility and value of personal data to all parties involved. The focus of current legislation reflects a tension between offering protection to the consumer and making the maximum use of the data. This "either-or" approach is evident in methods such as the opt-in/opt-out choice. Opt-in/opt-out is a fairly rudimentary mechanism. It does not allow for a fine-tuning of preferences in a way that would satisfy the consumer's need for selected information and the industry's need for making products and services known. Consider, for instance, a consumer's preference "do not disclose date of birth, unless it is to obtain a discount on a cruise to Norwegian fjords." Given only two choices the consumer would opt out of disclosure. Given a fine-tuned option, a consumer would more likely opt in. Both parties would benefit: the consumer saves time by not having to research cruise providers, and the cruise providers have access to an interested consumer without the need for a market study. In short, a fine-tuned solution allows for a very efficient matching process.

Third, a technology-based solution would give the data subjects greater control over its data and their use. The system's architecture would be implemented so as to provide the data subject realistic access and the opportunity to verify and correct. Although the "access/opportunity to correct" principle is an elementary requirement of the FIPs, in practice it is most often ignored.[134] This is largely due to the cost of

---

[134] Schwartz, *Health Care Information*, *supra* note 76; *see also* Schwartz, *Privacy and Democracy in Cyberspace*, *supra* note 76.

implementing a special architecture that permits such access in case of every collector or user.[135]

Below is an outline of several functions that could be assigned to a technological infrastructure as part of a comprehensive personal data privacy law.

A. The Technological Component – Collection, Transfer and Storage Of Data and Preference Information

Standardized methods for the electronic handling of personal data are not new.[136] One method developed for this purpose is the P3P protocol, for use in online transactions.[137] This protocol enables individuals to program their browsers to identify classes of information that they are willing or unwilling to disclose.[138] The negotiation would therefore take place at the browser level, and the individuals would not have to haggle over the terms and conditions with every site they visit.[139] Browsers can be programmed to avoid sites that do not comport with the individual's privacy preferences.[140] Although P3P has been subject to some criticism,[141] certain commentators believe that P3P will be an effective solution to the privacy problem.[142]

This may be true as far as online transactions between browsers are concerned. However, not all privacy violations occur online or are the result of online data collections. Of equal concern are the large quantities of data that derive from sources such as the DMV, the local grocery store or professional service providers, or data initially supplied voluntarily in the course of, and possibly in consideration of, an offline transaction. These data are collected in the normal course of business by many entities and then sold to aggregators, who combine them with the data collected online and sell them on to third parties.[143] Consequently, due to the high degree of integration of online and offline data, a comprehensive solution to the data problem must cover both online and offline transactions.

Because personal data are typically subject to numerous successive transfers, only a technological solution can ensure that the data remain permanently associated with a given set of preferences throughout the transfer. A possible approach would be to create an encrypted digital "envelope" which contains the data along with their attributes, i.e. the individual's preferences. Transfer of the digital envelope or of information contained therein, would be facilitated by a specially-designed protocol. To ensure that information contained in the envelope has not been tampered with, a digital signature could authenticate the envelope. The signature would be issued by

---

[135] *Id.*

[136] *See* Karen Coyle, *Pretty Poor Privacy? A Social Analysis of the Platform for Privacy Preferences* (June 1999), *at* http://www.kcoyle.net/p3p.html.

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] LESSIG, *supra* note 100, at 160.

[143] For instance, Direct Media, a mailing list broker in Greenwich, Conn., offers access to 2.9 million Lycos users at a cost of $125 per thousand names for a single mailing. An extra $15 per thousand lets marketers select users showing an interest in a certain topic. Saul Hansell, *"Privacy Policy on Web Shifts as Profits Ebb,"* THE N.Y. TIMES, April 11, 2002, at A1.

an information registrar or a certifying agency that could also serve as a source of re-verification of the authenticity of the attributes every time a new sale occurs.[144]

This protocol would likely be a component of a more comprehensive infrastructure. For instance, the data envelopes could be stored in personal data repositories that could be either centralized or distributed. These repositories could be general or organized by subject matter, e.g. financial information, health information, etc. A new user would obtain authorization to use the data from the data subject, but the data themselves would be released by the data repository. The repository would serve a function similar to that of a bank. Its operator would be responsible to A for the accuracy of data and to B and C for correctly carrying out the transaction itself. The repository containing the original and accurate data and attributes would certify each release of data to a new user. In addition to acting as a repository, the repository operator could also take the place of B and act as collector of information for sale to third parties.

Finally, the repository would electronically discharge the functions incident to the Fair Information Principles. A review of these principles[145] - notice, choice, access, onward transfer, data integrity and security[146] - reveals that their requirements are not only capable of, but are indeed suited to, execution by an automated system. Notice, choice and access are functions that require interaction with the data subject. They can easily be performed by a protocol which, upon receipt of certain instructions, sends out notices, receives and registers preferences and allows data subjects access upon proof of identity. The onward transfer principle is met by the mandatory norm imposed upon all collectors/users of data.[147] The principles of data integrity and security are quintessentially technological functions and require no interaction with the data subject. Their performance flows naturally from the infrastructure's security features.

Further details for the architecture supporting the technological infrastructure are beyond the scope of this paper and this author's sphere of competence, are best developed in conjunction with specialists in software programming and systems architecture.

B. The Legal Component: Norms of Conduct

1. Norms Governing the User's Conduct

Once the transfer of data and preferences is delegated to a technological infrastructure, the norms governing the conduct of data users easily falls into place.

---

[144] *See* Jonathan Weinberg, *Hardware-Based ID, Rights Management and Trusted Systems*, 52 STAN. L. REV. 1251, 1257 (2000) (describing one way of creating a secure infrastructure by means of a "trusted system").

[145] As articulated in the Safe Harbor formulation which is the most expansive of FIP versions.

[146] The FIP of "enforcement" is met via the mandatory norms which provide for availability of expedited and economically viable redress.

[147] *See infra* text accompanying notes 149-52.

The analogy that suggests itself is the doctrine of "encumbrances" to property in the law of real estate. This real estate doctrine was created to ensure that downstream transferees of real property are bound by certain pre-existing obligations incident to the property.[148] This is accomplished by obligations permanently associated with a piece of property intended "to bind the assigns of the covenantor and to vest in the assigns of the covenantee, in the same manner as if they had personally entered into them."[149] The obligations pass on extra-contractually in the form of a "covenant that runs with the land."[150] Originally a common-law norm, the covenant was subsequently codified[151] and provides that a transferee of real estate may, under given circumstances, acquire the property subject to the burden of the obligations incident to that particular property.[152]

This model is applicable to personal data as well. A "covenant that runs with the data" would serve as an extra-contractual method for binding downstream transferees. In practice, this solution would work as follows: a mandatory norm[153] would bind the data user to the data subject's preferences and compliance with the FIPs.[154] The user would be granted a license to use the data contained in the data subject's information "envelope" only in accordance with the limitations set forth therein. Access to the information itself would be gained through a data repository. A legislated provision of this nature would substitute for a contract between the data subject or transferor and transferee and would relieve the data subject and downstream transferees from having to pass on the obligations downstream.

The pendant to the covenant running with the land is a public notice function, which serves to inform the public of the existence and the nature of the encumbrance. Real estate law has established an elaborate structure of public notice via registration in a centrally-designated location, normally the County Recorder's office.[155] Its cost is supported by charging a small fraction of the value of real estate for each transaction. In the same way, a personal data repository would serve to provide notice of preferences, access to data subjects and to users, while being financed by a small fraction of the value of each transaction.

A legislated norm must further provide for an expedited and economically viable mechanism for redress of possible violations. This requires correcting the imbalance between the cost of enforcement and the potential recovery, which, if measured by

---

[148] *See* Martin v. Ray, 76 Cal. App. 2d 471 (1946).

[149] CAL. CIV. CODE § 1460 (2002).

[150] "Certain covenants, contained in grants of estates in real property, are appurtenant to such estates, and pass with them, so as to bind the assigns of the covenantor and to vest in the assigns of the covenantee, in the same manner as if they had personally entered into them. Such covenants are said to run with the land." CAL. CIV. CODE § 1460 (2002).

[151] *Id.*

[152] *Martin,* 76 Cal. App. 2d 471. "The burden imposed by the transaction is on the land conveyed and incident to its ownership. When grantees acquired the property it was taken subject to the burden; and the benefit of the covenants passed as incident of their ownership." *Id.*

[153] Mandatory rules are preset expressions of policy choices made by the legislature that cannot be waived or negotiated around. For a discussion of mandatory and default rules, see Schwartz, *Health Care Information, supra* note 76.

[154] *Id.*

[155] *Id.*

the value of the data, can be very low. Statutory damages[156] can serve both to compensate the victim and to deter against violations of the mandatory norms. From the procedural point of view, an expedited remedy for personal data transfer violations, including injunctive relief, is necessary to fully protect the data subject.

Finally, a mandatory norm should prohibit immoral commercial activities, such as misappropriation of personal data, unauthorized collection/use, stripping data of their identifiers or attributes, use of unauthenticated personal data, fraud, misrepresentation, or hacking into the encrypted envelope in which the data are stored.[157]

2. Norms Governing the Technological Component

Use of technology creates a new class of participants in the transaction, namely the data repository operator. Its role is to safeguard the data subjects' personal data and preferences and to vouch for the accuracy of the information. The obligations incident to these functions require imposition of fiduciary duties upon the repository operator.

Finally, a key issue is whether legislation should specify the parameters of the technological infrastructure. Since technological advances far outpace the ability of legislatures to pass laws, specification of a particular technology or even systems architecture is not indicated. Instead, the systems architecture and its functions are governed by the desired policy goals. The policy goals at issue for the present purposes are the Fair Information Principles.[158] Because discharge of the obligations incident to the FIPs is well suited for automated handling,[159] this function is in its entirety delegated to the technological infrastructure. To ensure that the desired policy goals are achieved, it is critical to incorporate the FIPs into the mandatory norms governing the technological component of a two-prong privacy legislation.[160]

CONCLUSION

An inherent tension exists between the individual's privacy interest and the data users' desire to maximize the commercial use of personal data. This tension continues to be an obstacle to enactment of comprehensive privacy legislation relating to personal data. Proposed legislation errs either on the side of favoring the

---

[156] These damages could be in the nature of the ones imposed by the Copyright Act. 17 U.S.C. § 504(c) (2002); Anticyberpiracy Act, 15 U.S.C. § 1125(d) (2002).

[157] J. Elford, *Trafficking In Stolen Information: A Heriarchy Of Rights Approach To The Private Facts Tort*, 105 YALE L.J. 727, 727 (1995).

[158] *See* discussion *supra* Part II.A.

[159] *See supra* text accompanying notes 146-47.

[160] An additional reason why this is important, is that the methodology selected for this technologically based solution, as well as its configurations and system design choices, are likely to have themselves a regulatory effect. *See* Schwartz, *supra* note 101, at 782. It is therefore very important to supplement this type of solution by a regulatory back-up that would ensure correct implementation of the desired public policy.

consumer, by imposing onerous burdens on the collector or user, or on the side of the collector or user, by providing inadequate privacy protection.

Both extremes stem from the fact that the quantity of data is, in practice, not manageable by traditional methods. Because the current unprecedented proliferation of data is due to technological developments, it makes sense to seek a solution that utilizes the capabilities of technology at the maximum level.

The present paper attempts to outline a legislative solution that relies heavily on the use of a technological infrastructure. The advantages it presents are that: (1) it affords enhanced privacy protection, by ensuring that all parties involved in data transactions honor the individual's privacy preferences; (2) data collectors or users are relieved of many of the onerous compliance requirements imposed by the Fair Information Practices, and (3) the value of personal data is maximized, for the benefit of both data subjects and users.

MICKEY MOUSE & SONNY BONO GO TO COURT: THE COPYRIGHT TERM EXTENSION ACT AND ITS EFFECT ON CURRENT AND FUTURE RIGHTS

VICTORIA A. GRZELAK

Cite as 2 J. MARSHALL REV. INTELL. PROP. L. 95