THE FAILURE OF FAIR INFORMATION PRACTICE PRINCIPLES

forthcoming in *Consumer Protection in the Age of the 'Information Economy'*

Fred H. Cate[1]

1. Introduction

Modern data protection law is built on "fair information practice principles" (FIPPS). At their inception in the 1970s and early 1980s, FIPPS were broad, aspirational, and included a blend of substantive (e.g., data quality, use limitation) and procedural (e.g., consent, access) principles. They reflected a wide consensus about the need for broad standards to facilitate both individual privacy and the promise of information flows in an increasingly technology-dependent, global society.

As translated into national law in the United States, Europe, and elsewhere during the 1990s and 2000s, however, FIPPS have increasingly been reduced to narrow, legalistic principles (e.g., notice, choice, access, security, and enforcement). These principles reflect a procedural approach to maximizing individual control over data rather than individual or societal welfare.

As theoretically appealing as this approach may be, it has proven unsuccessful in practice. Businesses and other data users are burdened with legal obligations while individuals endure an onslaught of notices and opportunities for often limited choice. Notices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical language, or they present no meaningful opportunity for individual choice. Trying to enforce notices no one reads has led in the United States to the Federal Trade Commission's tortured legal logic that such notices create enforceable legal obligations, even if they were not read or relied upon as part of the deal.

Moreover, choice is often an annoyance or even a disservice to individuals. For example, the average credit report is updated four times a day in the United States. How many people want to be asked to consent each time? Yet how meaningful is consent if it must be given or withheld for all updates as a group? How meaningful is a credit reporting system if individuals can selectively choose what to include and exclude? Most people appear to go out of their way to avoid making choices about information collection and use; if forced to, they are often ill-equipped to appreciate the risks either to our privacy or the benefits that may be lost if information is not available.

In addition, many services cannot be offered subject to individual choice. Requiring choice may be contrary to other activities important to society, such as national security or law enforcement, or to other values, such as freedom of communication. This explains why so many laws that purport to invest individuals with control over information about them exempt so many

[1]Distinguished Professor and Director of the Center for Applied Cybersecurity Research, Indiana University; Senior Policy Advisor, Center for Information Policy Leadership at Hunton & Williams. The author is grateful for the thoughtful comments of his colleagues, Peggy Eisenhauer and Marty Abrams, and for the excellent research assistance of Anne Tucker. The author alone is responsible for any errors that remain.

activities: it simply is not feasible or desirable to provide for individual control (or, in many cases, notice or access either).

Enforcement of notice, choice, and the other FIPPS is uneven at best. Individuals are rarely in a position to know if personal information about them has been used in violation of some prior notice that they received or consent that they gave. Situations likely to threaten greatest harm are often subject to the least oversight, while innocuous or technical violations of FIPPS may be prosecuted vigorously if they are the subject of a specific law or obligation and they can be used to generate popular or political pressure. This was documented by the disclosure during the first half of 2005 that tens of millions of business records containing personal information in the United States, Japan, and other countries had been hacked, stolen, or lost. Experts testified that this has been going on for years. Until these disclosures, however, regulators had addressed information security, part of all sets of FIPPS, only when privacy notices made representations about security that were later demonstrated to be untrue.[2]

In short, the control-based system of data protection, with its reliance on narrow, procedural FIPPS, is not working. The available evidence suggests that privacy is not better protected. The flurry of notices may give individuals some illusion of enhanced privacy, but the reality is far different. The result is the worst of all worlds: privacy protection is not enhanced, individuals and businesses pay the cost of bureaucratic laws, and we have become so enamored with notice and choice that we have failed to develop better alternatives. The situation only grows worse as more states and nations develop inconsistent data protection laws with which they attempt to regulate increasingly global information flows.

This chapter reflects a modest first step at articulating an approach to privacy laws that does not reject notice and choice, but does not seek to rely on it for all purposes. Drawing on other forms of consumer protection, in which standards of protection are not negotiable between providers and consumers, I propose that national governments stop subjecting vast flows of personal data to restraints based on individual preferences or otherwise imposing the considerable transaction costs of the current approach. Instead, I propose that lawmakers reclaim the original broader concept of FIPPS by adhering to Consumer Privacy Protection Principles (CPPPS) that include substantive restrictions on data processing designed to prevent specific harms.

The CPPPS framework is only a first step. It is neither complete nor perfect, but it is an effort to return to a more meaningful dialogue about the legal regulation of privacy and the value of information flows in the face of explosive growth in technological capabilities in an increasingly interconnected, global society.

2. The Evolution of Fair Information Practice Principles

According to Professor Paul Schwartz, a leading scholar of data protection law in the United States and Europe, "[f]air information practices are the building blocks of modern

[2]See, e.g., In the Matter of Eli Lilly and Company, FTC File No. 012 3214 (Jan. 18, 2002) (agreement containing consent order).

information privacy law."[3] Marc Rotenberg, president of the Electronic Privacy Information Center, has written that "Fair Information Practices" have "played a significant role" not only in framing privacy laws in the United States, but in the development of privacy laws "around the world" and in the development of "important international guidelines for privacy protection."[4] In fact, so important are these principles that Rotenberg writes of them only in capital letters, like one might write of the Bible or the Koran. What are FIPPS and from where did they originate?

a. The HEW Code of Fair Information Practices

In the early 1970s, mounting concerns about computerized databases prompted the U.S. government to examine the issues they raised—technological and legal—by appointing an Advisory Committee on Automated Personal Data Systems in the Department of Health, Education and Welfare. The Advisory Committee issued its report, *Records, Computers and the Rights of Citizens*, in 1973.[5] In that report, the Advisory Committee called on Congress to adopt a "Code of Fair Information Practices," based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for a person to find out what information about the person is in a record and how it is used.

3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.[6]

These principles may be described in more contemporary terms as reflecting five FIPPS: transparency, use limitation, access and correction, data quality, and security. They were the basis for the Privacy Act, which Congress adopted the following year.[7]

---

[3]Paul M. Schwartz, "Privacy and Democracy in Cyberspace," 52 *Vanderbilt Law Review* 1607, 1614 (1999). Professor Schwartz describes FIPPS as being "centered around four key principles: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight." Id.

[4]Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy: What Larry Doesn't Get," 2001 *Stanford Technology Law Review* 1 ¶ 43.

[5]U.S. Department of Health, Education and Welfare, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computer, and the Rights of Citizens* (1973).

[6]Id. at viii.

b. Privacy Protection Study Commission Principles

The Privacy Act created a Privacy Protection Study Commission to examine the wide range of privacy issues in greater detail. The Commission reported to President Carter in 1977.[8] Its report articulated three fundamental objects for any data protection system, and a number of specific recommendations for how those objectives might be achieved.

1. To create a proper balance between what an individual is expected to divulge to a record-keeping organization and what he seeks in return *(to minimize intrusiveness).*[9]

The Commission recommended that "that individuals be informed more fully than they now are of the information needs and collection practices of a record-keeping organization in advance of committing themselves to a relationship with it."[10] The reason was simple: "If the individual is to serve as a check on unreasonable demands for information or objectionable methods of acquiring it, he must know what to expect so that he will have a proper basis for deciding whether the trade-off is worthwhile for him."[11]

The Commission also recommended "that a few specific types of information not be collected at all."[12] The Commission's example—arrest information in "the employment and personnel area"—suggests that the real concern was use, rather than collection.[13]

The Commission proposed certain limitations on "information collection methods." "In general, the Commission believes that if an organization, public or private, has declared at the start its intent to make certain inquiries of third parties, and to use certain sources and techniques in doing so, it should be constrained only from exceeding the scope of its declaration."[14] The Commission also recommended that "private-sector record keepers be required to exercise reasonable care in selecting and retaining other organizations to collect information about individuals on their behalf."[15]

As a final step to minimize the intrusiveness of information gathering, the Commission recommended "having governmental mechanisms both to receive complaints about the propriety of inquiries made of individuals and to bring them to the attention of bodies responsible for

---

[7]The Privacy Act of 1974, 5 U.S.C. § 552a.

[8]The Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977).

[9]Id. at 14.

[10]Id. at 16.

[11]Id.

[12]Id.

[13]Id.

[14]Id.

[15]Id.

establishing public policy."[16] The Commission was quick to point out, however, "that such complaints require the most delicate public-policy response."[17] As a result, the Commission expressed a preference "to see such concerns addressed to the greatest possible extent by enabling the individual to balance what are essentially competing interests within his own scheme of values."[18]

2. To open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of it *(to maximize fairness)*.[19]

In the Commission's view, maximizing fairness required assuring that records about individuals "are as accurate, timely, complete, and relevant as is necessary to assure that they are not the cause of unfairness in any decision about the individual made on the basis of them."[20] This is best achieved, according to the Commission, by giving the individual the "right to see, copy, and correct or amend records about himself."[21] The Commission also noted that fairness "includes the responsibility to apprise individuals that records have or will be created about them, and to have reasonable procedures for assuring the necessary accuracy, timeliness, completeness, and relevance of the information in the records they maintain about individuals, including a responsibility to forward corrections to other organizations under specified circumstances."[22]

The Commission concluded that fairness was served in some situations by "requiring the individual's authorization" and by ensuring that a "disclosure should include no more of the recorded information than the authorized request for disclosure specifies."[23]

3. To create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual *(to create legitimate, enforceable expectations of confidentiality)*.[24]

The Commission recommended "that a legally enforceable 'expectation of confidentiality' be created in several areas." According to the Commission's report, the "concept of a legally enforceable expectation of confidentiality has two distinct, though complementary, elements."[25] The first is "an enforceable duty of the record keeper which preserves the record keeper's ability to protect itself from improper actions by the individual, but otherwise restricts its discretion to

[16]Id. at 17.

[17]Id.

[18]Id.

[19]Id. at 14-15.

[20]Id. at 17.

[21]Id.

[22]Id. at 18.

[23]Id. at 19.

[24]Id. at 15.

[25]Id. at 20.

disclose a record about him voluntarily."[26] The second is "a legal interest in the record for the individual which he can assert to protect himself against improper or unreasonable demands for disclosure by government or anyone else."[27]

The Privacy Protection Study Commission report reflects perhaps the broadest array of FIPPS in a U.S. context, although the breadth of those principles is mitigated somewhat by the fact that most would apply in only certain situations or where specified types of information were involved.

c. The OECD Guidelines

The HEW Code of Fair Information Practices and the report of the Privacy Protection Study Commission played a significant role in the development of the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* by the Committee of Ministers of the Organization for Economic Cooperation and Development in 1980.[28] The OECD Guidelines identified eight principles to "harmonise national privacy legislation and, while upholding such human rights, . . . at the same time prevent interruptions in international flows of data."[29] They were designed to "represent a consensus on basic principles which can be built into existing national legislation" and to "serve as a basis for legislation in those countries which do not yet have it."[30] In this aspiration they have undoubtedly succeeded because most of the dozens of national and regional privacy regimes adopted after 1980 claim to reflect the OECD Guidelines.

The Guidelines identified eight principles:

1. Collection Limitation Principle—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle—Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

[26]Id.

[27]Id. at 20-21.

[28]O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980).

[29]Id. at preface.

[30]Id.

4. Use Limitation Principle—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by the authority of law.

5. Security Safeguards Principle—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle—An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle—A data controller should be accountable for complying with measures which give effect to the principles stated above.[31]

Under the OECD Guidelines, data processors have certain obligations without regard for the wishes of individual data subjects. For example, the data quality and security safeguards principles appear non-negotiable. Other obligations are stated more broadly and may be affected by individual consent. For example, under the use limitation and purpose specification principles, the use of personal data is restricted to the purposes for which the data were collected, purposes "not incompatible with those purposes," and other purposes to which the data subject consents or that are required by law. Still other principles—for example, the openness and individual participation principles—are designed entirely to facilitate individual knowledge and participation.

The breadth of the OECD Guidelines' purposes (including both protecting privacy and facilitating multinational data flows), principles, and language, reflecting a real-world flexibility and proportionality, undoubtedly help explain their wide adoption and wide acclaim.

[31]Id. ¶¶ 7-15.

d. The EU Data Protection Directive Principles

In 1990 the Commission of the then-European Community published a draft *Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*.[32] The draft directive was part of the ambitious program by the countries of the European Union to create not merely the "common market" and "economic and monetary union" contemplated by the Treaty of Rome,[33] but also the political union embodied in the Treaty on European Union signed in 1992 in Maastricht.[34] The shift from economic to broad-based political union brought with it new attention to the protection of information privacy. After substantial amendment, the directive was formally approved on October 24, 1995.[35] Beginning three years later, each of the then-15 member states of the European Union were required to adopt national data protection laws in compliance with the directive's terms.

The directive is a long and detailed document, but it reflects a series of data protection principles that have been articulated by a "Working Party on the Protection of Individuals with regard to the Processing of Personal Data," composed of national data protection commissioners and charged under article 29 of the directive with interpreting key portions of the directive. According to the Working Party, the following principles are central to the directive:

1. The purpose limitation principle—data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. . . . [W]here data are transferred for the purposes of direct marketing, the data subject should be able to "opt-out" from having his/her data used for such purposes at any stage.

2. The data quality and proportionality principle—data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

3. The transparency principle—individuals should be provided with information as to the purpose of the processing and the identity of the data controller . . . , and other information insofar as this is necessary to ensure fairness. . . .

4. The security principle—technical and organizational security measures, should be taken by the data controller that are appropriate to the risks presented by the

[32]Com(92)422 Final SYN 287 (Oct. 15, 1992).

[33]Treaty Establishing the European Economic Community, Mar. 25, 1957, 28 U.N.T.S. 3, art. 2 (1958), as amended by the Single European Act, O.J. L 169/1 (1987), [1987] 2 C.M.L.R. 741, and the Treaty on European Union, Feb. 7, 1992, O.J. C 224/01 (1992), [1992] C.M.L.R. 719, reprinted in 31 I.L.M. 247 (1992).

[34]Treaty on European Union, Feb. 7, 1992, O.J. C 224/01 (1992), [1992] C.M.L.R. 719, reprinted in 31 I.L.M. 247 (1992).

[35]*Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Eur. O.J. 95/L281). See generally Christopher Kuner, *European Data Privacy Law and Online Business* (2003).

processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

5. The rights of access, rectification and opposition—the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. . . .

6. Restrictions on onward transfers—further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (*i.e.* the recipient of the onward transfer) is also subject to rules affording an adequate level of protection.[36]

7. Sensitive data—where "sensitive" categories of data are involved [data concerning "racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion . . . [or] concerning health or sexual life"[37]] additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

8. Automated individual decision—where the purpose of the transfer is the taking of an automated decision . . . , the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.[38]

Finally, two enforcement principles emerge from the directive. The first—the independent oversight principle—requires that entities that process personal data not only be accountable but also be subject to independent oversight. In the case of the government, this requires oversight by an office or department that is separate and independent from the unit engaged in the data processing. Under the data protection directive, the independent overseer must have the authority to audit data processing systems, investigate complaints brought by individuals, and enforce sanctions for noncompliance.[39]

The second enforcement principle—the individual redress principle—requires that individuals have a right to pursue legally enforceable rights against data collectors and processors who fail to adhere to the law. This principle requires not only that individuals have enforceable

[36]Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Working Document on Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (July 24, 1998).

[37]Directive, supra, art. 8.

[38]*Transfers of Personal Data to Third Countries*, supra.

[39]Directive, supra, art. 18.

rights against data users, but also that individuals have recourse to courts or a government agency to investigate and/or prosecute noncompliance by data processors.[40]

As discussed below, national legislation implementing the directive has tended to focus more on notice and consent than these principles suggest. Nevertheless, these ten principles mark the high-water mark of substantive legal protection for information privacy. Subsequent enactments in Canada, Japan, and other countries have followed similarly broad and substantive FIPPS.

e. The FTC Privacy Principles

Beginning in the mid-1990s, the Federal Trade Commission and states attorneys general encouraged U.S. operators of commercial websites to adopt and publish online privacy policies. Adoption of such policies was voluntary; compliance with them was not. The Commission interprets section five of the Federal Trade Commission Act, which empowers the FTC to prosecute "unfair and deceptive" trade practices, to include violations of posted privacy policies.[41]

In 1998, the FTC reported to Congress on what it believed a privacy policy must contain.[42] After reviewing the "fair information practice codes" of the United States, Canada, and Europe, the Commission concluded: "Common to all of these documents are five core principles of privacy protection:"

1. Notice/Awareness—The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles discussed below—choice/consent, access/participation, and enforcement/redress—are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.

2. Choice/Consent—The second widely-accepted core principle of fair information practice is consumer choice or consent. At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information—*i.e.*, uses beyond those necessary to complete the contemplated transaction.

3. Access/Participation—Access . . . . refers to an individual's ability both to access data about him or herself—*i.e.*, to view the data in an entity's files—and to contest that data's accuracy and completeness. Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass

[40]*Transfers of Personal Data to Third Countries*, supra.

[41]15 U.S.C. § 45(a)(1).

[42]Federal Trade Commission, *Privacy Online: A Report to Congress* 7 (1998).

timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.

4. Integrity/Security—[D]ata must be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.

5. Enforcement/Redress—It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles.[43]

The FTC's 1998 report is a remarkable landmark along the evolution of modern FIPPS for two reasons. First, it is noteworthy for having reduced prior collections of eight or ten principles down to five. (In 2000, the FTC issued a second privacy report to Congress which removed enforcement/redress, thereby reducing the list to four principles.[44]) Although this might be thought to reflect the FTC's focus, which was limited to website privacy policies, the Commission cites to the full range of FIPPS documents and identifies these five as the "core principles of privacy protection" that those documents have in common.

Second, it is striking that the chosen five (or four) principles were, with the exception of security, procedural. Substantive obligations concerning fairness and data quality were ignored in favor of procedural requirements concerning notice, choice, access, and enforcement. In terms of FTC law, the Commission was relying on its power to prohibit "deceptive" trade practices—i.e., practices that did not conform to published privacy policies—rather than its power to prohibit "unfair" trade practices.

f. The APEC Privacy Framework

The most recent set of FIPPS was adopted by the Asia-Pacific Economic Cooperation forum in 2004.[45] A conscious effort to build on the OECD Guidelines, but to modernize them in light of more than 20 years' experience and the escalating demand for standards that facilitate multinational data flows, the APEC Privacy Framework includes nine principles:

[43]Id. at 7-10 (citations omitted).

[44]Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* 11 (2000).

[45]Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, 2004/AMM/014rev1 (Nov. 2004). The author participated in drafting early versions of the framework for the U.S. government.

1. Preventing Harm—Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

2. Notice—Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information. . . . All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.

3. Collection Limitation—The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

4. Uses of Personal Information—Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: (a) with the consent of the individual whose personal information is collected; (b) when necessary to provide a service or product requested by the individual; or, (c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

5. Choice—Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.

6. Integrity of Personal Information—Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.

7. Security Safeguards—Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

8. Access and Correction—Individuals should be able to: (a) obtain from the personal information controller confirmation of whether or not the personal

information controller holds personal information about them; (b) have communicated to them, after having provided sufficient proof of their identity, personal information about them . . .; and, (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

9. Accountability—A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.[46]

The principles of the APEC Privacy Framework closely track the OECD Guidelines, however, with greater attention on notice and choice and a new principle—prevention of harm—added.

3. Fair Information Practice Principles in Operation

a. Which FIPPS?

As the preceding discussion suggests, one initial problem of basing a data protection regime on FIPPS is determining which set of FIPPS to apply. The OECD Guidelines provide eight, the EU data protection directive eleven, and the FTC principles only five (or four).

The differences are often quite substantive. For example, only the OECD Guidelines and APEC Framework provide an explicit collection limitation principle: "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[47] The EU data protection directive gets there obliquely, by defining "processing" to include "data collection" and then providing a purpose limitation principle to processing, but it is not a principle that the Article 29 Working Party considered "core." The other FIPPS, including the FTC principles, have no collection limitation principle at all: processors are free to collect whatever data they wish so long as they provide an accurate notice.

Similarly, the principle of openness or transparency is explicitly provided only in the OECD Guidelines, the HEW Code, and the EU data protection directive. There is no mention of it in the FTC principles or the APEC Privacy Framework. In those FIPPS, the broader goal of transparency has been reduced to mere notice. The data quality principle—the requirement that data be "accurate, complete, and up-to-date"—is completely missing from the FTC principles. The EU directive and the APEC Privacy Framework introduce entirely new principles that are found

[46]Id. at 8-19.

[47]OECD Guidelines, supra.

nowhere else: restrictions on onward transfers, special protection for sensitive data, limits on automated decision-making, and prevention of harm.

Finally, there are significant differences in terminology and levels of abstraction among the various FIPPS. What is the difference between "collection limitation," "purpose specification," and "use limitation," all three of which appear in the OECD Guidelines, and how do they compare with "purpose limitation" as that term is used to describe the EU directive? Does the latter include all three of the former? Some FIPPS, like the APEC Privacy Framework, provide considerable detail, but still rely on qualifying phrases such as "where appropriate." Others are considerably more vague.

The end result is significant differences among various sets of FIPPS, with the EU directive at one end of the spectrum, providing widespread limits on the processing of personal data with few countervailing interests explicitly acknowledged; the OECD Guidelines and APEC Privacy Framework in the middle, with explicit recognition of the need for balance and proportionality; and the FTC principles at the other end of the spectrum, with the fewest substantive restrictions (although perhaps the most rigorously enforced procedural ones) on data processors. Advocates of building national or regional data protection regimes based on FIPPS need to be careful to clarify which FIPPS they mean.

b. The Focus on Consumer Control

Many sets of FIPPS, and particularly those adopted since the OECD's 1980 guidelines, have been implemented to reflect a distinct goal of data protection as empowering consumers to control information about themselves, as opposed to protecting individuals from uses of information about them that are unfair or harmful. Alan Westin in his groundbreaking 1967 study, *Privacy and Freedom*, defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[48] By the 1990s, the focus on control had become the hallmark of data protection, especially in the United States, as aptly described by *New York Times* columnist William Safire: "excepting legitimate needs of law enforcement and public interest, control of information must rest with the person himself."[49]

This is not just a U.S. phenomenon and it is not entirely new. Multinational FIPPS have long reflected this focus, but it has grown in prominence in more recent sets of principles and in their application. For example, the OECD 1980 Guidelines provided that "[p]ersonal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by the authority of law."[50]

The EU data protection directive, as discussed in greater detail below, is significantly focused on individual choice. According to the directive, data protection is achieved through

[48]Alan F. Westin, *Privacy and Freedom* 7 (1967).

[49]William Safire, "Nosy Parker Lives," *New York Times*, Sept. 23, 1999, at A29.

[50]OECD Guidelines, supra at ¶ 7.

substantive "obligations imposed on persons . . . responsible for processing," and through "the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances."[51]

By the adoption of the APEC Privacy Framework in 2004, the focus on choice was unmistakable. It is evidence in many of the principles, and especially the choice principle: "Were appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information."[52]

All of these data protection instruments reflect the same approach: tell individuals what data you wish to collect or use, give them a choice, grant them access, secure those data with appropriate technologies and procedures, and be subject to third-party enforcement if you fail to comply with these requirements or individuals' expressed preferences. All of these elements serve individual choice and each is meaningless without that choice. For example, what good is notice or access if the individual has no control over the information? Professor Schwartz has described this focus as "privacy-control":

> Most scholars, and much of the law in this area, work around a liberal paradigm that we can term "privacy-control." From the age of computer mainframes in the 1960s to the current reign of the Internet's decentralized networks, academics and the law have gravitated towards the idea of privacy as a personal right to control the use of one's data.[53]

c. The Focus on Notice and Choice

The most immediate evidence of the migration from substantive rules for data protection to procedural steps for enhancing individual control is the fact that in the past two decades most FIPPS have been applied in practice to require primarily notice and, in some instances, choice. This is especially clear in the United States, where the FTC first narrowed the OECD's eight principles down to five—notice, choice, access, security, and enforcement—and then later abandoned enforcement as a "core" principle.[54] Describing notice as "the most fundamental principle," the FTC has focused virtually all of its privacy-related efforts on getting websites to post privacy policies and its enforcement efforts on suing website operators when they fail to follow those policies.

What is immediately striking about the FTC's approach is not only its exclusion of most FIPPS, but also its transformation of collection limitation, purpose specification, use limitation, and transparency into mere notice and consent. Under the former principles, personal data may

---

[51]EU Data Protection Directive, supra, Preamble, ¶ 25.

[52]APEC Privacy Framework, supra at 12.

[53]Schwartz, supra at 1659.

[54]FTC, *Privacy Online* (2000), supra.

only be collected by "lawful and fair means," may only be used for the purposes for which they were collected and other compatible purposes, and must be handled under a "general policy of openness about development, practices and policies."[55] Consent is relevant only as a usual condition for data collection and as an exception to the use limitation principle (i.e., personal data may be used for other purposes with the consent of the data subject). The other conditions are non-negotiable.

The FTC's approach reflects more than its awareness of the importance of the market economy and the role that personal information plays in it,[56] and more than just the limits imposed on regulating information by the First Amendment.[57] It reflects a materially different orientation towards data protection than that of earlier FIPPS. For example, the FTC's approach eliminates the requirements that data collection be "fair," that data not be used for incompatible purposes, and that data processing operations generally be open. Moreover, the FTC's approach, as discussed in further detail below, reduces notice and consent to a mere formality—a checkbox that consumers must select to obtain a desired product or service. By treating disclosures as legal notices, the FTC's approach infects them with legal technicalities and minutia appropriate for a contract but not for a consumer disclosure. The Commission's approach allows the notice to contain virtually anything, irrespective of how unfair or unrelated its provisions may be. Most importantly, it has substituted procedural protections, which have often proved ineffective, for substantive ones, such as the consumer protection standards it applies in other areas.

U.S. statutes and regulations have tended to follow or parallel the FTC's control-based approach. For example, in 1999 Congress passed major financial privacy legislation as Title V of the Gramm-Leach-Bliley Financial Services Modernization Act.[58] Ironically, Title V contains only three substantive restrictions on the use of personal information: prohibitions on sharing account numbers with third parties for marketing purposes, on pretext calling, and on transfers of personal information to third parties for marketing purposes if the data subject has opted out.

The real focus of the new law is on procedural requirements. The law permits a financial institution to transfer any "nonpublic personal information" to nonaffiliated third parties only if the institution "clearly and conspicuously" provides consumers with a notice about its information disclosure policies and an opportunity to opt out of such transfers.[59] That notice must be sent at least annually even if there is no change in its terms. The act provides many exceptions to the notice and consent requirements when, for example, the use of information is necessary to provide a product or service requested by a customer, protect against fraud or other liability, or comply with applicable laws.[60]

---

[55]OECD Guidelines, supra.

[56]FTC, *Privacy Online* (1998), supra at 3-4. See generally Fred H. Cate, *The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It*, The Freedom Forum (2003).

[57]See Fred H. Cate & Robert Litan "Constitutional Issues in Information Privacy," 9 *Michigan Technology & Telecommunications Law Review* 35 (2002).

[58]Gramm-Leach-Bliley Financial Services Modernization Act, 106 Pub. L. No. 102, 113 Stat. 1338 (1999).

[59]Id. § 503(b).

[60]Id. §§ 502(b)(2), (e).

As this example suggests, notice and choice statutes often provide consumers with few meaningful choices. Gramm-Leach-Bliley, in fact, allows for just one: consumers can opt out of some, but not all, transfers of personal information to third parties for marketing purposes. As a practical matter, therefore, consumers' only serious choice in response to the legally required notices is to choose to take their business elsewhere, assuming there is another financial institution that discloses preferable data processing practices.

A second example of the focus on notice and, to a lesser degree, choice is found in the rules for protecting the privacy of personal health information adopted in 2001 by the Department of Health and Human Services, under the Health Insurance Portability and Accountability Act.[61] As amended in 2002,[62] the rules regulate the use of information that identifies, or reasonably could be used to identify, an individual, and that relates to physical or mental health, the provision of health care to an individual, or payment for health care.[63] The rules apply to "covered entities," namely, anyone who provides or pays for health care in the normal course of business, and, indirectly, to anyone who receives protected health information from a covered entity.[64]

A covered entity may use personal health information to provide, or obtain payment for, health care only after first providing the patient with notice and making a good faith effort to obtain an "acknowledgment."[65] Notices must meet detailed requirements set forth in the rules; proof of providing notice and acknowledgments must be retained for six years after the date on which service is last provided.[66]

A covered entity may use personal health information for most purposes other than treatment or payment only with an individual's opt-in "authorization."[67] An "authorization" must be an independent document that specifically identifies the information to be used or disclosed, the purposes of the use or disclosure, the person or entity to whom a disclosure may be made, and other information.[68] A covered entity may not require an individual to sign an authorization as a condition of receiving treatment or participating in a health plan.[69]

A covered entity may use or disclose personal health information for directories and to notify and involve other individuals in the care of a patient if the covered entity obtains the

---

[61]Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (2000) (HHS, final rule) (codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

[62]Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 43,181 (2002) (HHS, final rule) (codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506). The unofficial text of the final rule as amended may be found at http://www.hhs.gov/ocr/combinedregtext.pdf.

[63]45 C.F.R. § 164.504.

[64]Id.

[65]45 C.F.R. § 164.506(a).

[66]Id. § 164.105(c)(2).

[67]Id. § 164.508(a)(1).

[68]Id. § 164.508(c).

[69]Id. § 164.508(a)(2)(iv).

"agreement" of the individual.[70] An agreement need not be written, provided that the individual is informed in advance of the use and has the opportunity to opt out of any disclosure.[71]

The health privacy rules thus provide more opportunities for consumer consent than the financial privacy provisions, but many uses of personal health information do not require consent. Even the ones that do are subject to a number of exceptions, under which personal health information may be disclosed, usually to government agencies, with neither consent nor authorization.[72] The health privacy rules well illustrate the growing complexity of notice and consent requirements: one rule to deal with the use of one type of information requires the use of three different types of notice and consent.

The focus on notice and consent is not limited to the United States. Despite the considerably broader array of data protection principles identified in the EU data protection directive, the directive and national laws within Europe transposing it have tended to focus on notice and consent. For example, article 7 of the directive provides seven conditions under which personal data may be processed. The first is "the data subject has unambiguously given his consent."[73] Article 8 restricts the processing of sensitive data, but then provides that the restriction shall not apply where "the data subject has given his explicit consent to the processing of those data."[74] Article 10 lays out the detailed information that must be given to the data subject before personal data are collected from him or her; article 11 provides for the same notice to be provided when data are collected from a third party. Article 14 covers the withdrawal of consent by the data subject. Article 26 identifies six exceptions to the provision prohibiting the export of personal data to non-European countries lacking "adequate" data protection. The first is that "the data subject has given his consent unambiguously to the proposed transfer."[75]

It is simply not accurate to say, as some EU officials have recently tried to do, that the directive is not concerned with notice and consent. By its own terms, it plainly is. Many of its substantive protections can be waived with consent. Moreover, it has been applied in practice to focus on notice and consent. Some national data protection authorities have tried to reduce the role of consent by arguing that consent cannot be freely given in certain circumstances, such as employment relationships. This creates an ironic conundrum: a data protection law that conditions data processing on consent and an enforcement mechanism that questions whether consent is possible. This facilitates neither individual choice nor the flow of information that are among the directive's intended goals.

d. Many Notices that Few People Read

[70]Id. § 164.510.

[71]Id.

[72]Id. § 164.512.

[73]EU Data Protection Directive, supra at art. 7(a).

[74]Id., art. 8(2)(a).

[75]Id., art. 26(1)(a).

The result of the focus on notice and consent in U.S., European, and other laws has been an avalanche of notices and consent opportunities. The irony is that they are widely ignored by the public. There are many explanations.

First, the notices may never be received. In fact, most requests for consumer consent never reach the eyes or ears of their intended recipient. According to the U.S. Postal Service, 52 percent of unsolicited mail in this country is never read.[76] Similar figures are reported by companies about the rates at which their marketing e-mail are opened by consumers. For example, one of the United States' largest on-line service providers indicated in 2002 that 58 percent of its marketing e-mails sent to its own customers were never opened.[77]

In 1997, U.S. West (now Qwest Communications), one of the largest telecommunications companies in the United States, tested a variety of methods for seeking consent from its customers to use information about their calling patterns (e.g., volume of calls, time and duration of calls, etc.)—to market new services to them.[78] In the trial of outbound calls, U.S. West found that it took an average of 4.8 dialing attempts to reach a live respondent with authority to consent. Of all the residential customers that U.S. West attempted to contact, 55 percent never received the offer or request for consent, even after multiple calling attempts.[79]

Second, the available evidence indicates that individuals tend to ignore privacy policies and consent requests if they can. The chief privacy officer of Excite@Home told an FTC workshop on profiling that the day after *60 Minutes* featured his company in a segment on Internet privacy, only 100 out of 20 million unique visitors to its website accessed that company's privacy pages.[80] According to an independent research firm's analysis, an average of .3 percent of Yahoo users read its privacy policy in 2002. Even at the height of the publicity firestorm created in March 2002 when Yahoo changed its privacy policy to permit advertising messages by e-mail, telephone, and mail, that figure rose only to 1 percent.[81] This is by no means limited to privacy notices. It appears to be true of most mandated disclosures, whether medical informed consent forms, mortgage disclosure forms, or license terms on software packages and splash screens.

---

[76]"Briefs," *Circulation Management*, May 1999 (referring to the U.S. Postal Service's *Household Diary Study* (1997)).

[77]Declaration of Fred H. Cate, Bank of America v. Daly City, 279 F. Supp. 2d 1118 (N.D. Cal. 2003), at 2.

[78]Ex parte letter from Kathryn Krause to Dorothy Attwood (Sep. 9, 1997), In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended, 63 Fed. Reg. 20,326 (1998) (FCC, second Report and Order and Further Notice of Proposed Rulemaking). U.S. West calculated that the trial had a margin of error less than 2 percent. Brief for Petitioner and Intervenors at 16 n.37, U.S. West v. FCC, 182 F.3d 1224 (10th Cir. 1999), cert. denied 528 U.S. 1188 (2000).

[79]Brief for Petitioner and Intervenors, id. at 10-11.

[80]Federal Trade Commission, Workshop on the Information Marketplace: Merging and Exchanging Consumer Data, Mar. 31, 2001 (comments of Ted Wham).

[81]Saul Hansell, "Compressed Data: The Big Yahoo Privacy Storm That Wasn't," *New York Times*, May 13, 2002, at C4.

Third, even when privacy notices are received, the evidence suggests they usually fail to provoke any significant response—positive or negative. The difficulty of prompting any response from consumers was clearly demonstrated by the lack of response to the Gramm-Leach-Bliley financial privacy notices. Under that law, by July 1, 2001, the tens of thousands of "financial institutions" to which it applies had mailed approximately 2 billion or more notices.[82] If ever consumers would respond, this would appear to be the occasion: The notices came in an avalanche, the press carried a wave of stories about the notices, privacy advocates trumpeted the opt-out opportunity and offered online services that would write opt-out requests for consumers, and the information at issue—financial information—is among the most sensitive and personal to most individuals.

By mid-August 2001, fewer than 5 percent of consumers had opted out of having their financial information shared with third parties. For many financial institutions, the response rate was lower than 1 percent.[83] A late September survey revealed that 35 percent of the 1001 respondents could not recall even receiving a privacy notice, even though the average American had received a dozen or more.[84] Extensive experience with company-specific and industry-wide opt-out lists suggests that this is not atypical. The lack of consumer response to Gramm-Leach-Bliley prompted then-FTC Chairman Timothy Muris to comment at the end of 2001:

> The recent experience with Gramm-Leach-Bliley privacy notices should give everyone pause about whether we know enough to implement effectively broad-based legislation based on notices. Acres of trees died to produce a blizzard of barely comprehensible privacy notices. Indeed, this is a statute that only lawyers could love—until they found out it applied to them.[85]

Privacy scholar Amitai Etzioni has noted that European citizens rarely, if ever, are asked for explicit permission to use personal information about them. In fact, he tells of regularly asking his European audiences if anyone has ever been asked to opt-in. Etzioni reports only one positive response—from a man who was asked for opt-in consent by Amazon.com, a U.S. company.[86]

The difficulties of reaching and provoking a response from consumers are greatly exacerbated where the party wishing to use the information has no (and may not have ever had) direct contact with the consumer. For example, most mailing lists are obtained from third parties. For a secondary user to have to contact every person individually to obtain consent to use the names and addresses on the list would cause delay, require additional contacts with consumers, and almost certainly prove prohibitively expensive. And it could not be done without using the very information that the secondary user is seeking consent to use.

---

[82] *Hearing on Financial Privacy and Consumer Protection*, Senate Comm. on Banking, Housing, and Urban Affairs, 107th Cong. (Sept. 19, 2002) (statements of Fred H. Cate and John Dugan).

[83] "Survey: Compliance with GLB Act Costs Smaller Banks More Money," *Consumer Financial Services Law Report*, Feb. 14, 2002.

[84] Star Systems, *Financial Privacy: Beyond Title V of Gramm-Leach-Bliley*, 2002, p. 9.

[85] Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Privacy 2001 Conference, Oct. 4, 2001.

[86] Fred H. Cate, *Opt-In Exposed*, American Banker's Association (2002), at 10.

e. Notices that Few People Understand

Many observers have noted that privacy policies are often difficult to understand. There is good reason for this. Because the FTC and states attorneys general have determined to treat notices as binding contracts, the people who draft them are understandably worried about being precise and inclusive. Moreover, as data protection laws and regulations become more complex, so do the notices required by those enactments.

It should also be noted that there is real disagreement about what makes a good privacy notice. On June 18, 2001, at a hearing on financial privacy of the California General Assembly's Committee on Banking and Finance, the Committee Chairman distributed American Express' privacy notice and challenged the financial services industry representatives in the audience to live up to the standard set by this "model." Two weeks later, on July 9, 2001, *USA Today* editorialized in favor of clearer privacy notices, citing American Express' notice—the same notice lauded only two weeks earlier—at its first example of a notice that was difficult to comprehend.[87]

As a result, privacy notices in the United States have become long and complex. In fact, eBay counsel Kent Walker has written that notices often suffer from:

- "Overkill"—"masses of unintelligible small print that no one bothers to read."[88]
- "Irrelevance"—describing activities of so little concern to most consumers that it "is like leading a satiated horse to unappealing water."[89]
- "Opacity"—reflecting the "bedrock truth . . . that it is difficult to track, let alone describe, all the information that is exchanged in a typical transaction, all the places that it is stored, and all the ways that it is used."[90]
- "Non-comparability"— again reflecting an underlying reality that "the simplification necessary for comparability comes at a significant cost in accuracy and flexibility."[91]
- "Inflexibility"—failing to keep pace with "new business models and new consumer demands."[92]

The problems with the current approach to notices will only expand as data protection laws are applied to new technologies, such as mobile phones, and computer chips embedded in cars and

[87]"Confusing Privacy Notices Leave Consumers Exposed," *USA Today*, July 9, 2001, p 13A.

[88]Kent Walker, "The Costs of Privacy," 25 *Harvard Journal of Law & Public Policy* 87, 107 (2001).

[89]Id. at 108.

[90]Id. at 110.

[91]Id. at 111.

[92]Id. at 112.

household appliances: Where will the "clear and conspicuous" privacy notice be displayed then? "The likely outcome," as the U.S. experience has amply demonstrated, is that "privacy policies will produce information that is unread by Americans and does not affect behavior and will result in the enrichment of the plaintiffs' bar with no benefits to consumers."[93]

The European experience has proved no more successful. Notices under European data protection laws are often reduced to mere warnings. One popular privacy notice throughout London and other European capitals is "Warning: CCTV in use." These signs may motivate good behavior, but they do little to empower individuals to make informed choices about the collection and use of data about them. Similarly, many European businesses provide brief privacy notices, often of obvious data collection practices (e.g., "if you reply to this e-mail we will collect personal data about you"). One British theater ticket service now offer callers the option to opt out of hearing its privacy notice altogether.

Neither approach—loading notices with exceptional detail because they will serve as contract terms or reducing notices to mere cigarette-pack-like warnings—has proved very informative or protective of privacy.

f. The Cost of Choice

The opportunity, much less the requirement, to make choices can impose considerable burdens on consumers, as well as on businesses seeking consent. U.S. West reported that it required an average of 4.8 telephone calls per household just to find an adult who could consent. Moreover, these additional contacts were just to obtain permission to examine data about customers to determine their eligibility for a product or service offering. For those individuals who are eligible, a second round of contacts is necessary to actually make them the offer. For the majority of people who will not qualify for the offer, the contacts were wasted.

A case study of MBNA Corporation, a large, diversified, multinational financial institution currently being acquired by Bank of America, provides even more striking examples.[94] MBNA uses personal information to pare down its lists of prospects in an average year from 800 million to 400 million names.[95] If consent were required, the company would have to contact 800 million people permission to scrutinize data about them, even though only 50 percent will qualify to receive an offer. The other 50 percent of contacts will have been wasted. This means, on average, 400 million Americans would hear from MBNA annually asking for permission to consider them for an offer for which they are ineligible.

Alternatively, if the company is prohibited from using personal information because of the inherent difficulty and cost of obtaining opt-in consent from distant consumers, 109 million people each year would receive solicitations who should not have.[96] These wasted contacts translate into

[93]Id. at 113.

[94]Michael E. Staten & Fred H. Cate, "The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA," 52 *Duke Law Journal* 745 (2003)

[95]Id. at 771.

[96]Id. at 775.

an 18 percent lower response rate and a 22 percent increase in direct mail costs per account booked—costs that are likely to be passed on to consumers in the form of higher prices.[97]

Consumers may also be burdened by receiving no contacts. In its telephone trial, U.S. West never reached 26 percent of its customers and was hung up on without ever being able to seek opt-in consent by another 28 percent. Fifty-four percent of the trial population were therefore denied opportunities to receive information about new products and services.[98] When compared with the 72 percent who opted-in when the opportunity to consent was presented at the conclusion of a call that the customer initiated, it is likely that many of those customers who never knew of the offer might in fact have been interested in it. The greatest impediment to securing consent wasn't that customers did not want their information used, but rather that they never learned of the opportunity or didn't like intrusive or repetitive contacts that the consent requirement necessitated.

Consumers bear other burdens as well, in addition to repetitive and wasteful contacts. Robert E. Litan, Director of the Economic Studies Program at The Brookings Institution and a former Deputy Assistant Attorney General, has written that mandatory consent requirements would "dramatically change the way goods and services are marketed in this country, whether 'on' or 'off' line. The same would be true for fund-raising by charitable and public interest organizations, many of which now purchase customer lists from magazines and other organizations (commercial and non-commercial)."[99]

"In all of these cases," Litan writes, "organizations would have to painstakingly build solicitation lists from scratch, a task that would be prohibitively expensive for all but the very largest commercial entities in the country. One result would be to raise barriers to entry by smaller, and often more innovative, firms and organizations."[100]

The impact may be measured in more than just wasted dollars and time. Consider medical research, where researchers performing chart review will likely have had no prior contact with the patient, and the patient will likely no longer be present in the health care system. To require that the researcher obtain the patient's consent means that the researcher will not only face all of the burdens normally associated with reaching individuals and getting them to respond to a consent request, but the additional burden of having to do so without the benefit of an existing relationship or a ready mechanism for communicating with them.

There is also a financial cost to notice and consent regulation. One component of that cost results from the interference of privacy laws with open information flows. Ultimately, it is consumers and individuals, in the words of then-Alabama Attorney General Bill Pryor, who "pay the

[97]Id.

[98]Brief for Petitioner and Intervenors, supra at 15-16.

[99]Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates,* AEI-Brookings Joint Center for Regulatory Studies Working Paper 99-3, at 11 (1999).

[100]Id.

price in terms of either higher prices for what they buy, or in terms of a restricted set of choices offered them in the marketplace."[101]

Another source of that cost is the burden of complying with notice and choice laws. Crafting, printing, and mailing the two billion disclosure notices required by Gramm-Leach-Bliley, for example, is estimated to have cost $2-5 billion.[102] Much of that cost will be incurred annually because the notices must be distributed annually. During its test of consent mechanisms, U.S. West found that to obtain permission to use information about its customer's calling patterns to market services to them cost almost $30 per customer contacted.[103]

These costs are not limited to business users of information. A 2002 study by Michael Turner and Lawrence Buc calculates that the annual cost to charities of complying with privacy laws requiring explicit consent for the use of personal information in fund-raising would be $16.5 billion—21 percent of the total amount raised by U.S. charities in 2000.[104]

g. The Benefits of No Choice

In some cases, consent may be undesirable, as well as impractical. This is true of press coverage of public figures and events, medical research, and of the many valuable uses of personal information where the benefit is derived from the fact that the consumer has not had control over the information. This is certainly true of credit information: its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make the credit report useless.

In the words of former FTC Chairman Muris: The credit reporting system "works because, without anybody's consent, very sensitive information about a person's credit history is given to the credit reporting agencies. If consent were required, and consumers could decide—on a creditor-by-creditor basis—whether they wanted their information reported, the system would collapse."[105]

Moreover, many of these beneficial uses of information that consumers now enjoy and to which they have the opportunity to consent, depend on spreading the cost of collecting and maintaining the information over a variety of uses. For example, commercial intermediaries collect and organize government records, and make them accessible to the public. Those records are used for many socially valuable purposes: monitoring government operations, locating missing children, preventing and detecting crime, apprehending wanted criminals, securing payments from "deadbeat" parents and spouses, and many others.

---

[101]Bill Pryor, *Protecting Privacy: Some First Principles*, Remarks at the American Council of Life Insurers Privacy Symposium, July 11, 2000, Washington, DC, at 4.

[102]*Hearing on Financial Privacy and Consumer Protection*, supra (statement of Fred H. Cate).

[103]Brief for Petitioner and Interveners, supra at 15-16.

[104]Michael A. Turner & Lawrence G. Buc, *The Impact of Data Restrictions on Fund-raising for Charitable & Nonprofit Institutions* 2-3 (2002).

[105]Muris, supra.

If the law restricted the other valuable uses of public records, or made those uses prohibitively expensive, then the data and systems to access them would not be in place for any use. Inasmuch as the beneficial uses of information outlined above are interconnected, and often depend on common systems and spreading the cost of acquiring and managing data over many uses, consent-based laws may lead to consumers having fewer opportunities made available to them to which they can consent.

h. The Illusion of Choice

Notice and consent requirements often create the illusion, but not the reality, of meaningful consumer choice. For example, if the notice is never received by the consumer, the choice it provides is meaningless. Conversely, if consent is required as a condition for opening an account or obtaining a service, a high response rate can always be obtained. A useful example are the license terms that computer users encounter when downloading or installing software. The first window that opens during the installation process is a notice of terms and conditions, usually relating to intellectual property rights. The user is given two options "I Accept" or "I Decline." Because the installation stalls until the individual makes a choice, it is not difficult to get him or her to make that choice. Moreover, because clicking on the "I Decline" button will terminate the installation process, it is not difficult to prompt the user to choose "I Accept." Software manufacturers could accurately claim a 100 percent consent rate to their license terms, but only because consent is a condition of service.

Financial institutions confronted with explicit consent laws report similar results. For example, one of the United States' largest financial institutions has reported that it has no difficulty complying with consent requirements in European countries, because it prints the opt-in notice in the account-opening form above the signature line. A consumer cannot open an account without granting consent.[106] "One's clicking through a consent screen to signify surrendering of her personal data for all future purposes is an example of both uninformed consent and a bad bargain."[107]

Finally, if the cost of obtaining consent becomes too great to make the proposed use of information economically feasible, then there will be nothing to which the consumer can consent. Similarly, if consent requires building new data systems, and implementing new uses of data, one person at a time, it is likely to make the activity untenable. For example, if a European company had to obtain the informed, affirmative consent of each of its employees in order to process its payroll in a non-European country, the existence of a single hold-out would mean that the company needed to provide an alternative payroll service, something few employers could afford. When that happens, consent requirements create only the illusion, not the reality, of choice. As Professor Schwartz has argued, "social and legal norms about privacy promise too much, namely data control, and deliver too little."[108]

[106]Cate Declaration, supra at 7.

[107]Schwartz, supra at 1678.

[108]Id. at 1677.

i. National Law in a Global World

The idea behind FIPPS was that national data protections laws would be compatible because they would be built on commonly shared principles. As a result, privacy would be protected without impeding global information flows. This was the explicitly stated purpose behind the OECD Guidelines, the EU data protection directive, and the APEC Privacy Framework.

The reality has been quite different. Implementation of these and other FIPPS has been so divergent that national laws are often incompatible, they often impose explicit barriers to the international flow of personal data, and they are increasingly supplemented by state, provincial, and even local data protection laws. As a result, data protection has grown inconsistent and unpredictable, and increasingly burdensome to multinational commerce, trade, and information flows.

This is most surprising in Europe, which adopted the data protection directive to create a uniform standard of data protection across the 15 member states of the European Union so that "personal data should be able to flow freely from one Member State to another."[109] The text of the directive stresses this point by forbidding member states from restricting the flow of personal data among themselves because of data protection or privacy concerns. But the directive explicitly restricts data flows to non-European countries lacking "adequate" data protection, and it allows member states to enact laws that provide greater data protection internally. The result is wide variation in the laws of European countries. A 2001 study by London law firm D.J. Freeman found that almost every member state "was operating its own regime in terms of data laws" with "wide latitude in the interpretation of the 1995 directive."[110] The end result of applying national choice-based data protection laws in the context of an increasingly global society has been called "a maze of conflicting provisions that create a complex, perilous, and potentially non-navigable environment" for consumers and businesses.[111]

The United States, as we have seen, has largely reduced the OECD Guidelines to four principles—notice, choice, access, and security. As a result, its data protection laws are already widely divergent from those of most other countries. In addition, because of the federal structure of the government, privacy protection varies widely state to state and even from city to city. While the federal government has recently imposed national statutory or regulatory protections for privacy of financial and health information, these explicitly permit state governments to adopt more restrictive provisions.

Privacy is increasingly cited as the reason for restricting multinational information flows. Concerns about privacy protections in other countries have been raised in debates over outsourcing in the United States, Canada, and elsewhere. The Canadian province of British Columbia has gone so far as to adopt a law prohibiting public sector outsourcing of the processing

[109]Directive, preamble, ¶ 3.

[110]"ASPs Warn: EU Data Protection Laws Fail to Keep Pace With Technology," *Business Wire*, March 6, 2001.

[111]*Hearing on the EU Data Protection Directive*, supra (statement of Jonathan Winer).

of personal information outside of Canada.[112] Specifically, the law requires each public body to ensure that "personal information in its custody or under its control is stored only in Canada and accessed only in Canada."[113]

Such inconsistency burdens consumers, who travel, shop, use credit cards, and engage in a variety of transactions from state to state and country to country. It also saddles businesses with the cost of identifying which data protection regime applies to a given act of data processing, understanding the requirements of that regime, and then applying them appropriately, and the risk of liability if they fail to reconcile inconsistent data protection requirements appropriately. The problem is especially true online. The Internet crosses state and national boundaries and has facilitated truly global markets, yet the technologies of the Internet often make it impossible to identify in which state or country users are located. The price of inconsistent data protection laws is borne by entities that must comply with those laws and by individuals whose privacy is supposed to be protected by them.

j. The Distortion of Privacy

The greatest failure of FIPPS as applied today is the substitution of maximizing consumer choice for the original goal of protecting privacy while permitting data flows. As a result, the energy of data processors, legislators, and enforcement authorities has been squandered on notices and often meaningless consent opportunities, rather than on enhancing privacy. Compliance with data protection laws is increasingly focused on providing required notices in proper form and at the right time, rather than on ensuring that personal information is protected.

Of the hundreds of enforcement actions brought in Europe, the United States, and other countries, few have involved allegations of substantive harms to individuals, while most have alleged failures to comply with procedural requirements. Meanwhile, serious risks to consumers, such as the apparent widespread insecurity of personal data, have gone largely unexamined.

This is a powerful indictment of modern data protection law, and it requires not just tinkering with notice and choice requirements or rethinking enforcement strategies. It requires rethinking the purpose of data protection law and reexamining the principles on which that law is based.

4. A Modest Proposal

Fair Information Practice Principles have failed in practice. Data protection regimes built on them are not delivering a high standard of effective, predictable, and efficient data protection, or meaningful consistency among nations or regions. Most importantly, as transposed into contemporary privacy laws and regulations, FIPPS have been used to glorify individual choice as if that, and not appropriate privacy protection, were the goal of data protection. While privacy

[112]Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, British Columbia, 2004.

[113]Id. § 30.1. See also Information and Privacy Commissioner of British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (Oct. 2004)

advocates and policymakers cling tenaciously to FIPPS, at least in their rhetoric, the reality is that FIPPS as applied today largely disserve both privacy and other important societal interests.

Creating an alternative that works better than FIPPS—whether returning to earlier FIPPS that did not substitute control for privacy, or identifying new alternatives—is a difficult undertaking because it requires settling on not only a more rational data protection regime, but one that can ultimately prove acceptable to a wide variety of people in very different national settings. This is the critical task to which this final section attempts to make a modest contribution.[114]

The following Consumer Privacy Protection Principles are intended to operate on two levels. At the higher level, they are designed to help guide the development of a data protection system and determine the appropriate role of law. At the more detailed level, they are intended to define what the key elements of data protection laws should be.

The first three principles establish the purpose of, and constraints on, data protection and therefore provide the standards for interpreting the other principles and guiding their implementation.

1. Prevention of Harm—Data protection laws should regulate information flows when necessary to protect individuals from harmful uses of information. Like other consumer protection laws, data protection law should be designed to prevent tangible harms to individuals and to provide for appropriate recovery for those harms if they occur. Tangible harms are defined as damage to persons or property.

    a. Focus on Use—Data protections laws should target harmful uses of information, rather than mere possession, and should focus on collection only to prevent collection by dishonest or deceptive means. Individuals are less likely to be harmed by the mere collection, possession, or transfer of accurate information. Moreover, even information that could be used for harmful purposes may also have uses that are beneficial for the data subject, the data user, and society as well.

    b. Proportionality—Data protection should be proportional to the likelihood and severity of the possible harm(s).

    c. Per Se Harmful Uses—Where a use is always harmful (e.g., the use of personal information to commit fraud), the government should prohibit the use outright.

    d. Per Se Not Harmful Uses—The government should not regulate uses that present no reasonable likelihood of harm.

[114]For another example of pragmatic thinking about privacy principles, which has influenced the recommendations below, see Fred H. Cate, Margaret P. Eisenhauer & Christopher Kuner, "A Proposal for a Global Privacy Protection Framework," *Consumer Protection Update*, American Bar Association 18 (Sum. 2003).

e. Sensitive Uses—Where a use of personal data is neither "per se harmful" nor "per se not harmful," the government may condition the use on obtaining the consent of the data subject(s). Such requirements should be reserved for uses of personal data:
   i. that are reasonably and objectively thought to be intrusive, offensive, or otherwise invade personal privacy;
   ii. where the intrusion, offense, or other objection is directly related to the use of personal data; and
   iii. where consent likely would be effective.

2. Benefits Maximization—Data protection is not an end in itself, but rather a tool for enhancing individual and societal welfare. To be effective, data protection must rest on the recognition that both information flows and individual privacy have value and are necessary in a democratic society and market economy. That value benefits individuals as well as society as a whole. Therefore, the goal of any privacy regime must be to balance the value of accessible personal information with the value of information privacy to maximize both individual and public benefits.

   a. No data protection law should be enacted or enforced that does not in fact significantly serve the purpose for which it was enacted. Laws that are ineffective or that are enacted without a specific purpose run the risk of imposing costs without achieving benefits.

   b. Data protection laws should not be enacted or enforced if they are substantially more burdensome or broader than necessary to serve that purpose. Such laws by definition impose costs in excess of the benefits they achieve. Similarly, some data protection laws, even if narrow and precise, may necessarily impose costs that exceed their benefits.

3. Consistent Protection—Individuals should enjoy privacy protection that is as consistent as possible across types of data, settings, and jurisdictions.

   a. Data protection laws should reflect broadly accepted, rational principles.

   b. To facilitate consistency and predictability in data protection, governments should avoid inconsistent or overlapping local laws or regulations, or overlapping enforcement actions.

   c. Where possible, data protection laws should be adopted at the highest practical level (e.g., national instead of local or provincial), and laws should be harmonized to the greatest extent possible in an effort to achieve consistent, if not uniform, national standards.

   d. Data protection laws should not impose special burdens on the transborder flow of personal data and should not create special or greater obligations outside of the jurisdiction in which the law operates than apply within the jurisdiction. Rather than seeking to impose extraterritorial legal obligations on data flows in other

countries, national data protection laws and authorities should focus instead on mutual recognition of concurrent national regimes. Compliance with the data protection laws of one country should satisfy the requirements of all other national laws that are based on the same principles.

The remaining principles describe in broad terms the legal obligations of data protection:

4. Transparency, Honesty, and Accountability—Entities should collect, use, or transfer personal data honestly and only in compliance with applicable law and with any stated or reasonably implied undertakings.

    a. Personal data should be collected from data subjects openly. If the collection from data subjects is not reasonably obvious, then there should be prominent notice of the fact. If data collection is reasonably obvious, additional notice requirements are superfluous.

    b. Entities that collect personal data to complete a transaction or provide a product or service requested by an individual should (i) collect and use no more information than is reasonably necessary, and (ii) use or transfer that information in the future only for compatible purposes.

    c. If personal data are collected or used based on the consent of the data subject, consent may not be required as a condition of providing a product or service unless the information is actually necessary for that purpose.

    d. Personal data should be collected from third parties only in compliance with applicable law and with any stated or reasonably implied undertakings by the third party to the data subject and by the entity seeking the data to the third party. If the data are used in any manner that could reasonably cause tangible harm to the data subject, the data subject should be provided with notice as to the source, content, and use of the data.

    e. Entities should be accountable at law for their use of personal information and for the activities of entities that process data on their behalf.

5. Integrity of Personal Information—Personal information should be accurate, complete and kept up-to-date consistent with how it is used. The level of accuracy, completeness, and timeliness should reflect the likelihood that the information could be used to cause harm and the severity of the likely harm.

6. Security—Personal data which could reasonably be used to harm individuals should be secured against accidental or deliberate loss, misuse, alteration, or destruction. The level of security should reflect the likelihood that the information could be used to cause harm and the severity of the likely harm. Legal requirements concerning security should be technology-neutral and avoid interfering with the development and use of new measures.

7. Liability—Entities that collect and otherwise process personal information should be liable for reasonably foreseeable actual damages resulting from their harmful use or misuse. Such entities should be liable only if the harm results from their negligent, willful, or intentional behavior. Liability should never be determined under a strict liability standard, or when the harm was not reasonably foreseeable or could not reasonably have been prevented.

8. Effective and Efficient Enforcement—Enforcement of data protection laws should achieve effective compliance with these principles and applicable law, as efficiently as possible, while minimizing the burden on individuals or interference with the benefits they enjoy.

    a. The goal of enforcement should be to achieve a high degree of compliance and to compensate victims for actual harms suffered as a result of misuse of personal information, without imposing unnecessary burdens on individuals or the responsible, lawful use of personal information.

    b. It is important that enforcement not create a disincentive for attempting to comply with the law, by unfairly focusing on responsible users who try and fail or by ignoring harmful uses of data that may be more difficult to prosecute. Enforcement actions should target information processors that contribute directly and materially to the harmful use of personal information.

    c. Data protection laws should not permit overlapping or duplicative enforcement actions. Enforcement should be as efficient as possible. To that end, governments should seek to avoid duplicative or overlapping enforcement actions.

Collectively, CPPPS are intended to focus data protection on those situations where it is most necessary, but to ensure that in those situations, the law will provide substantive protections, not merely hollow notices and opportunities for consent. They are designed to provide individuals with sufficient notice of data processing activities and sufficient protection so that they can make intelligent, self-reliant decisions, but not to use those decisions as a substitute for substantive protection where needed. And they are calculated to provide sufficient, targeted liability so that data processors will have meaningful incentives, rather than pages of bureaucratic regulations, to motivate appropriate behavior, and that individuals will be compensated when processing results in serious harm.

This approach reflects other provisions of consumer protection law, particularly the focus on tangible harms, the requirement of some form of causality or requirement before liability is found, and the reliance on substantive rather than procedural protections. For example, fraud law in the United States typically requires (1) false representation of material fact; (2) knowledge by the seller that the information is false; (3) intent for buyer to rely upon false information, (4) reasonable reliance on behalf of the buyer; and (5) injury resulting from the buyer's reliance on the

false information.[115] But liability flows when these conditions are found. As a general matter, consumers cannot consent to be defrauded and notice of intent to defraud is not a defense.

The CPPPS also reflect elements of the Fair Credit Reporting Act, which on notice and consent only in a limited way and with regard to specific activities.[116] Instead, the Act restricts the use of consumer report information to statutorily specific "permissible purposes," and imposes strict requirements on furnishers and users of that information concerning its accuracy. It is not a perfect model and is certainly too bureaucratic and restrictive for many uses of information that present little risk to individuals, but it is a useful example.

Privacy law is not unique. It is important and it touches on many values—including both privacy and the free flow of information—that civilized societies carry about, but it can certainly be informed by other sources of law that also deal with important values. Experience in those analogous areas might help us not only formulate more workable principles, but also translate them into law more faithfully and consistently.

5. Conclusion

Modern privacy law is often expensive, bureaucratic, burdensome, and offers surprisingly little protection for privacy. It has substituted individual control of information, which it in fact rarely achieves, for privacy protection. In a world rapidly becoming more global through information technologies, multinational commerce, and rapid travel, data protection laws have grown more fractured and protectionist. Those laws have become unmoored from their principled basis, and the principles on which they are based have become so varied and procedural, that our continued intonation of the FIPPS mantra no longer obscures the fact that this emperor indeed has few if any clothes left.

We can do better. The key is refocusing FIPPS on substantive tools for protecting privacy, and away from notice and consent; leveling the playing field between information processors and data subjects; and created sufficient, but limited, liability so that data processors will have meaningful incentives, rather than bureaucratic regulations, to motivate appropriate behavior, and that individuals will be compensated when processing results in serious harm. This is only a first step. These proposed Consumer Privacy Protection Principles are undoubtedly incomplete and imperfect, but they are an effort to return to a more meaningful dialogue about the legal regulation of privacy and the value of information flows in the face of explosive growth in technological capabilities in an increasingly global society.

---

[115] See Gene A. Marsh, *Consumer Protection Law in a Nutshell* (1999).

[116] 15 U.S.C. ‘ 1681b.