



# Privacy and Fair Information Practices

---

THE STRUGGLE TO PROTECT  
THREATENED VALUES

**JIM HARPER**

APRIL 2021

A M E R I C A N   E N T E R P R I S E   I N S T I T U T E

# Executive Summary

---

For 50 years, the concept of fair information practices (FIPs) has dominated debates about privacy protection. FIPs are sets of organizational rules meant to protect people's privacy. Ideally, if corporations and governments collected, retained, shared, and used personal information according to such guidelines, people would have privacy even while they interacted with these large institutions. FIPs are so ingrained that for many they have become synonymous with privacy.

There have been many different versions of FIPs, and the way FIPs are expressed can differ in important ways. Many FIPs are so general and contextual that they provide little real guidance, and some FIPs

conflict with others. FIPs vacillate between embracing consumer choice and prescription.

Most importantly, FIPs unevenly address the full range of values that advances in information technology threaten in this burgeoning Information Age. FIPs focus mostly on fairness and privacy (as control of others' access to information), with a secondary focus on satisfying anti-commercial preferences. FIPs only indirectly and derivatively protect values such as personal and financial security, peace and quiet, autonomy, and reputation.

Legislation based on FIPs has not solved the privacy problem and cannot be expected to. Other modes for responding to Information Age challenges may better protect privacy and related values.



# Privacy and Fair Information Practices

---

## THE STRUGGLE TO PROTECT THREATENED VALUES

**Jim Harper**

We are in a time of profound and rapid change. Information technology is infiltrating every dimension of life, vastly improving things for people while unsettling them by upending many institutions, habits, and expectations. The present era of change may not be as profound as the development of agriculture or the rise of cities, but today's changes are happening much faster. Agriculture grew over millennia and the rise of cities over hundreds of years. The information revolution rivals the Industrial Revolution, which occurred over most of a century.

In the past, people adopted new technologies and varied their modes of living over generations. Small accretions and erosions of legal and social institutions could accommodate the changes. As transportation and trade began to flourish in preindustrial Europe,<sup>1</sup> for example, legal recognition for movable property developed as a supportive social structure. William Blackstone mentioned that development briefly in his *Commentaries on the Law of England*.<sup>2</sup>

Today's rapid change is testing the capacity of our legal and social systems to absorb it. This is true in many dimensions of human endeavor. Consider ongoing, intense controversies about the media and whom people should trust for information about matters of public interest.<sup>3</sup> Platform-based work challenges the modern convention that most people will funnel their skills and labor through a single employer.<sup>4</sup> But today especially we are suffering acute discontinuity in the collection and use of information about us—in our privacy.

What should be done?

What policymakers and governments have done is a logical exercise that lays out certain rules of behavior for information-gathering institutions: fair information practices (FIPs). These rules ideally would protect human values or mitigate effects on them while allowing the benefits of technology to flourish. It is hard to be satisfied that the privacy regulations modeled on FIPs do those things.

Blackstone cataloged and thus solidified English law in the 18th century, providing a resource for the adoption of English legal traditions and common law in the new United States of America. It might be odd to identify a Blackstone for modern privacy protection, but for this report, I select a pioneer analyst of computing and its social consequences.

Willis Ware was an engineer at the RAND Corporation who foresaw much about the extent of computing and its relevance to people's lives. "The computer will touch men everywhere and in every way, almost on a minute-to-minute basis," he wrote in a 1966 paper presented at RAND. "Every man will communicate through a computer whatever he does. It will change and reshape his life, modify his career, and force him to accept a life of continuous change."<sup>5</sup> For men and women alike, Ware contributed a great deal to the social and legal response.

FIPs are sets of rules that organizations can follow to protect people's privacy. At least that is the aspiration. Ideally, corporations and governments would

collect, retain, share, and use personal information according to proper guidelines. And if they did so, people would have their privacy even while they interacted with these giant administrative machines.

For the past 50 years, FIPs have been the dominant modality for privacy protection. They frame US sectoral regulation aimed at privacy, including the US federal government outside of law enforcement and national security. Europe has adopted FIPs-based regulation for its entire private economy.

Without diminishing the work of Ware, who remained a student of privacy well into his later years,<sup>6</sup> it is hard to say that FIPs-oriented privacy protection has been a success. There is no measuring privacy to see if there is enough, but 50 years along, privacy still seems under threat. Where FIPs-based regulation has been adopted, it has not relieved the stress on privacy. The European Union is on its second round of FIPs-based regulation. Such regulation is complex and costly. Resistance to it inspired by its negative effects on economic growth and innovation has been easier because the benefits of regulating are unclear.

---

## **There is no measuring privacy to see if there is enough, but 50 years along, privacy still seems under threat.**

The history of the FIPs shows sincere efforts to protect privacy among countless individuals in numerous organizations, legislatures, and bureaucracies globally. Over the decades, there have been many versions of FIPs. They vary and oscillate in concept and emphasis. That is probably because the interests under threat today include not just privacy (as control over others' access to information) but also fairness, personal and financial security, peace and quiet,

autonomy, reputation, and integrity against commodification, or anti-commercialism.<sup>7</sup>

Protective responses are needed in this era of advancing information technology and changing business models. But there is a jagged intersection between FIPs and the many values under threat. FIPs-based legislation aimed at solving the "privacy" problem in one fell swoop seems unlikely to do so. Privacy and these other values might be better protected by responses oriented to human interests rather than logically derived principles.

### **The Founding of FIPs**

Willis Ware had an idea. He wanted to inform people about how the financial services industry collects, retains, shares, and uses personal data. It was September 29, 1972, and the Secretary's Advisory Committee on Automated Personal Data Systems was having its sixth meeting. Most meetings lasted two or three days. After two more meetings that year, the committee would review a draft of its findings at its final meeting in 1973.

"Suppose you had applied for a loan application, or a deposit account," Ware said to a panel of financial services industry executives, "and you filled out the necessary forms, but prior to your signing it, the clerk took out a card and read you something like the following:

"You are hereby informed that as a result of the information you are about to give, one, this information will be entered into a computer-based system.

"Two, as prescribed by law, this data will be automatically passed to certain other computer-based systems; notably, the IRS.

"Three, this information will be subject to the process of inspection.

"Four, for reasons of business of this institution, it will be made available to credit reference bureaus.

"Five, other than as specifically noted above, this institution has no control over further dissemination.

"Your signature on this application constitutes acknowledgement that you have been informed of these facts."

It was a rough summary of what happened to people's financial information then and what still happens today.

"Now, if this were done," Ware asked, "would you find this objectionable in your business, do you think there would be deleterious effects? Would you expect some reaction from your customers?"<sup>8</sup>

The Secretary's Advisory Committee on Automated Personal Data Systems was an early and highly influential panel commissioned by the US Department of Health, Education, and Welfare. It investigated computerized data use in business, government, and society. Its conclusions, issued in 1973 with Ware as chairman, recommended legislation establishing a "code of fair information practice" for all automated personal data systems.

The "HEW report," as it came to be called, recommended a new legal code that would provide civil and criminal penalties for any unfair information practice. People objecting to unfair information practices could seek injunctions to stop them. Individual or class action lawsuits arising from unfair information practices would allow plaintiffs to seek actual, liquidated, and punitive damages and the recovery of attorneys' fees and other costs of successful suits.<sup>9</sup>

What defects, pitfalls, and dangers in the world of personal information would such legislation and lawsuits address? The HEW report recited the following principles of fair information practice:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.

- 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 misuse of the data.<sup>10</sup>

The HEW report was not the first to recommend principles like these. The Committee on Privacy in the UK, chaired by Sir Kenneth Younger, issued conclusions the year before, including a list of 10 principles.<sup>11</sup> But the HEW report arrived as the Watergate scandal was consuming Washington, DC, and its conclusions supplied the framework for reform legislation that passed soon after. The Privacy Act of 1974<sup>12</sup> was based on eight principles according to the Privacy Protection Study Commission established by that law.<sup>13</sup> FIPs have anchored privacy policy discussions ever since.<sup>14</sup>

## Privacy's essential nature may require FIPs rather than simpler and more direct codes of conduct. Part of that is privacy's individual subjectivity.

The concept of FIPs was inspired partly by unfair labor practices: actions taken by employers or unions that are illegal under the National Labor Relations Act (NLRA) and other US labor laws.<sup>15</sup> But FIPs are not a code like the NLRA. Instead, FIPs are high-level statements. Sometimes they are referred to as "practices" and sometimes "principles"—two different things—and sometimes they are referred to as "fair information practice principles."<sup>16</sup>

There is some reason for this gravitation to high-level statements rather than clear rules. Privacy's essential nature may require FIPs rather than

simpler and more direct codes of conduct. Part of that is privacy's individual subjectivity. Privacy "rests on a conception of society as comprising relatively autonomous individuals," say Colin J. Bennett and Charles D. Raab in *The Governance of Privacy: Policy Instruments in Global Perspective*. "Individuals, with their liberty, autonomy, rationality, and privacy, are assumed to know their interests, and should be allowed a private sphere untouched by others."<sup>17</sup> This premise seems valid, if only because others are *even worse* at knowing and protecting people's interests than are individuals themselves.

Another premise Bennett and Raab identify is that the better mode for protecting privacy is government regulation. People cannot suitably protect privacy in markets because "personal information cannot easily be regarded as a property right,"<sup>18</sup> say Bennett and Raab. They echo widespread consensus in scholarly, policymaking, and regulatory circles by stating, "It is very difficult to establish personal information as property in law, and then to define rights in action over its illegitimate processing."<sup>19</sup> This premise might be worth reconsidering, if only because of the unsatisfactory privacy outcomes under the regulatory approach of the past half century. Courts have increasingly recognized privacy notices as contracts, suggesting privacy may indeed be a private good that people can secure as they wish through legal relationships.<sup>20</sup>

These two premises interact. If privacy is an interest that varies among individuals and communities, regulations that address privacy cannot be prescriptive. Instead, Bennett and Raab find, privacy policy "is based inevitably . . . on *procedural*, rather than *substantive*, tenets."<sup>21</sup> Procedures such as those Ware proposed would encourage consumers to define their interests themselves according to context. At least, that was the hope.

In modern privacy parlance, the FIPs in the HEW report boil down to transparency, use limitation, access and correction, data quality, and security.<sup>22</sup> The list of FIPs has expanded and contracted over time as different organizations have added and subtracted FIPs, sometimes disentangling the conceptually dense ones.

The Organisation for Economic Co-operation and Development (OECD), for example, produced *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980 to harmonize national legislation and "prevent interruptions in international flows of data."<sup>23</sup> The document was heavily influenced by its FIPs forbears, and it in turn heavily influenced later legislation. It identified eight principles to "serve as a basis for legislation in those countries which do not have it yet."<sup>24</sup> Obligations set down in the Council of Europe Convention No. 108 the following year were "not dissimilar" from those included in the OECD guidelines or guidelines issued by the UN in 1990, according to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, a group formed by the EU data protection directive in 1995.<sup>25</sup>

Work on the EU's first effort—the 1995 data protection directive—began in 1990 under the Commission of the European Communities. A meta-statute requiring each EU member state to adopt national data protection laws, it included:

- "Principles related to data quality,"
- "Criteria for making data processing legitimate,"
- A section dedicated to "special categories of processing,"
- Requirements for "information to be given to the data subject,"
- "The data subject's right of access to data,"
- "The data subject's right to object," and
- Other terms and requirements.<sup>26</sup>

In a document related to transfers of personal data to non-EU countries, the working party summarized the directive as having eight FIPs-like principles.<sup>27</sup>

In two places, the EU data protection directive deviated from process-based rules, instead focusing

on harm prevention. Among its 72 “whereas” clauses, it stated, “Any damage which a person may suffer as a result of unlawful processing must be compensated for by the [data] controller.” And in its substantive sections, it required EU member states to provide that “any person who has suffered damage as a result of an unlawful processing operation . . . is entitled to receive compensation.”<sup>28</sup> These provisions have been little noticed, though harm control appeared again in later FIPs-based documents.

In 1998, the US Federal Trade Commission (FTC) issued a report that was notable for the relatively small number of FIPs it asserted. The FTC identified five “widely-accepted principles concerning fair information practices” that it said were common to the preceding documents.

1. **Notice and Awareness.** “Consumers should be given notice of an entity’s information practices before any personal information is collected from them.”
2. **Choice and Consent.** “Choice means giving consumers options as to how any personal information collected from them may be used.”
3. **Access and 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.”
4. **Integrity and Security.** “Data [must] be accurate and secure.”
5. **Enforcement and Redress.** “Privacy protection can only be effective if there is a mechanism in place to enforce [it]. . . . Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.”<sup>29</sup>

The FTC report eschewed the talk of human rights found in European reports, focusing on the utilitarian benefits of increased trust. Without privacy protections, it said, “electronic commerce will not reach its full potential.”<sup>30</sup> It also emphasized risks to children’s privacy, including lack of parental consent for children’s interactions, and it called for legislation addressing that subject. Congress passed such legislation later in 1998 with the Children’s Online Privacy Protection Act.<sup>31</sup> In a subsequent report, the FTC eliminated the enforcement and redress FIP, thus reducing its list from five to four principles.<sup>32</sup>

The Asia-Pacific Economic Cooperation (APEC) forum adopted the next important set of FIPs in 2004.<sup>33</sup> The *APEC Privacy Framework* led with an added, somewhat unique directive focusing on preventing harm. “Personal information protection,” its first principle stated, “should be designed to prevent the misuse of such information. . . . Remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.”<sup>34</sup> This was an important conceptual step, as it suggested an alternative to rote FIPs compliance by asking what uses of personal information are harmful.

Finally, in 2016, the European Union revised its previous directive, issuing a new General Data Protection Regulation (GDPR), which took effect in 2018. The heart of the GDPR, Article 5, is a recitation of seven FIPs.

1. Personal data shall be:
  - a. processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);
  - b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be

considered to be incompatible with the initial purposes (“purpose limitation”);

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; [subject to exceptions] . . . (“storage limitation”);

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).<sup>35</sup>

A month after the May 2018 effective date of the GDPR, California passed a new law, the California Consumer Privacy Act. It, too, has many elements of the FIPs.<sup>36</sup>

So we arrive at FIPs 50 years along and firmly entrenched in some important jurisdictions. Have FIPs succeeded? Nobody can say. Social science experiments rarely have controls, so we do not know how privacy protection would look or how much privacy and other values people would enjoy had world regulatory history taken another course.

We can improve on the science, though, and move to a more granular understanding of FIPs by examining

them in relation to the values they may protect. For a better idea of whether FIPs are good, we can assess what ends they serve and how they are meant to work.

## What Do FIPs Do?

The HEW report and FIPs initiatives that followed are clear examples of deductive privacy problem-solving. FIPs rely on expertise and logic to determine what ills exist in the digital world and how to protect people from them. Experts like Willis Ware, examining the digital world unfurling before them, anticipated many problems and suggested many solutions.

Ware’s notice regime for financial services was meant to inform people of some data sharing and some of the uses made of personal information while they made key financial decisions. We cannot know what precise goals Ware had in mind when he proposed this. If we knew his goals, it would still be hard to determine how well his notice regime would achieve them. But we can fairly assume he was seeking to protect consumers from certain ills. The same is true of FIPs authors since.

FIPs are so ingrained that for many “they have become synonymous with privacy,” according to Northeastern University privacy law and computer science professor Woodrow Hartzog.<sup>37</sup> But the word “privacy” means a lot of different things. In 1980, the OECD said in introducing its FIPs, “There has been a tendency to broaden the traditional concept of privacy (‘the right to be left alone’) and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.”<sup>38</sup> And maybe that is not all FIPs cover. My study finds that the values at stake include eight values:

**1. Control of Others’ Access to Personal Information.** For countless reasons, including having a sense of control, people prefer to keep some information about themselves from others. This is the essence of privacy, and I refer to it as “privacy” in this report.



2. **Fairness.** It is important that each individual should get their due, whether that is opportunity and promotion or punishment and loss.
3. **Personal Security.** Denying others information about oneself can protect against physical threats and violence.
4. **Financial Security.** Information can be a tool of financial frauds such as “identity theft,” in which someone impersonates another, creating accounts and debts in the victim’s name.
5. **Peace and Quiet.** People want to enjoy a sense of retreat from the world.
6. **Autonomy.** The availability of information about people is an essential tool of legal and social pressure that may restrict people’s freedom to act.
7. **Integrity Against Commodification.** Many resist what seems to be the commercialization of everything and prefer to be treated as whole individuals.
8. **Reputation.** People worry that negative information about them will create negative impressions and adverse social and economic treatment.<sup>39</sup>

To get a better handle on how FIPs may protect these values, let us now examine how FIPs and values interrelate. First we must select a universe of FIPs to analyze. In 2006, Bennett and Raab identified 10 fair information principles they believed were a matter of “strong consensus.”

1. **Accountability.** An organization “must be *accountable* for all the personal information in its possession.”
2. **Purpose Identification.** An organization “should *identify the purposes* for which the

information is processed at or before the time of collection.”

3. **Knowledge and Consent.** An organization “should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances).”
4. **Minimal Collection.** An organization “should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes.”
5. **Limited Use and Disclosure.** An organization “should not use or disclose personal information for purposes other than those identified, except with the consent of the individual.”
6. **Limited Retention.** An organization “should *retain* information only as long as necessary.”
7. **Data Quality.** An organization “should ensure that personal information is kept *accurate, complete, and up-to-date*.”
8. **Security.** An organization “should protect personal information with appropriate *security safeguards*.”

9. **Openness.** An organization “should be *open* about its policies and practices and maintain no secret information system.”

10. **Access and Correction.** An organization “should allow data subjects *access* to their personal information, with an ability to amend it if it is inaccurate, incomplete, or obsolete.”<sup>40</sup>

Below I examine how these practices logically and theoretically intersect with the values I identified above, noting which values are primarily served

by which FIP. It is a messy and imperfect process, roughly summarized in Table 1. Many FIPs are so general and contextual that they provide little real guidance. Some FIPs conflict with others. Many FIPs directly affect a given value while derivatively affecting many others, all depending on context. FIPs vacillate between embracing consumer choice and prescription. Any set of FIPs may lack elements or emphases of another set. The way FIPs are expressed can differ in important ways. Flaws in the set of FIPs analyzed below may be corrected in another set. But the availability of a “no true Scotsman” argument—explaining that a better FIPs version answers any challenge—may reveal just how malleable the FIPs tradition is.

The analysis shows, though, that FIPs mainly serve two values: fairness and privacy (as control of others’ access to information). Fairness is as important as information control is. FIPs do not address the other values threatened by burgeoning information technology as much as one might expect, though FIPs offer a lot for those who are concerned with the overcommercialization of life. That might be FIPs’ topmost secondary focus.

Comparing FIPs to values moves us closer to an articulate discussion of how legislation or regulation based on FIPs serve or fail to serve given values. Confounding the analysis slightly, though, the first FIP Bennett and Raab identify is a highly general sort of “meta-FIP.”

**Accountability.** Because people are not angels, accountability is an essential force for good behavior. Wrongdoers should be punished, and right-doers should be rewarded. As a general principle, accountability is entirely sound.

But it is very general. Metaphysically, all individuals and organizations are accountable to others. In many ways, all depend on others for sustenance and maintenance, which can be withdrawn. Thus, the accountability FIP begs some important questions: To whom must an entity be accountable? What is the best mix of accountability mechanisms among government regulation, litigation, market forces, or others? (Is it important for accountability to motivate adherence

to FIPs versus other influences such as habit or morals and ethics?)

The HEW report’s proposed legislative FIP code would have exposed wrongdoers to criminal enforcement and lawsuits seeking injunctions and damages. That was a proposal for accountability via litigation, based on rights created by legislation. As sources of enforcement and redress, the FTC identified legislation creating private remedies (i.e., lawsuits), “regulatory schemes enforceable through civil and criminal sanctions,” and “industry self-regulation.”<sup>41</sup> The source of accountability implied in many FIPs and preferred by many FIPs advocates is administrative regulation. That is, violation of legislative or regulatory rules based on FIPs should expose wrongdoers to government investigations and civil penalties.

---

**The accountability FIP  
begs some important  
questions: To whom must  
an entity be accountable?  
What is the best mix of  
accountability mechanisms  
among government  
regulation, litigation,  
market forces, or others?**

A mechanism designed for market accountability is the self-regulatory certification, which may play some role in signaling privacy trustworthiness. A 2016 study found that 27 percent of internet privacy policies across numerous sectors cited compliance with third-party guidelines in their privacy policies, though not all actually comply.<sup>42</sup> These

**Table 1. Summary of How FIPs Affect Values**

	Control of Access	Fairness	Personal Security	Financial Security	Peace and Quiet	Autonomy	Integrity Against Commodification	Reputation
Accountability	Accountability is a meta-FIP that lets various forms of oversight protect all values.							
Purpose Identification	Positions privacy-sensitive to exercise access control	DC	DC	DC	DC	DC	DC	DC
Collection with Knowledge and Consent	Positions privacy-sensitive to exercise access control	DC	DC	DC	DC	DC	DC	DC
Limited Collection to Where Necessary for Purpose	Restricts access to information even when not sought using the purpose identification and knowledge and consent FIPs	DC	DC	DC	DC	DC	DC, MBA	DC, MBA
Limited Use and Disclosure	Enforces limits on sharing established through the purpose identification and knowledge and consent FIPs	DC	DC	DC	DC	DC	DC	DC
Retention Only as Long as Necessary	Limits access along the time dimension	MBA		MBA		A bias against retention helps thwart legal and social pressure.	A bias against retention helps satisfy anti-commercial instincts.	
Data Kept Accurate, Complete, and Up-to-Date (Data Quality)	MBA	Accuracy aids fairness.					Accuracy soothes some anti-commercial concerns.	Accuracy aids in reputation assessment.

(Continued on next page)

Table 1. Summary of How FIPs Affect Values (Continued)

	Control of Access	Fairness	Personal Security	Financial Security	Peace and Quiet	Autonomy	Integrity Against Commodification	Reputation
Security Safeguards	Limits data breach and thus loss of control	May limit data corruption and thus wrong decisions	Limits data breach and thus may limit personal security risks	Limits data breach and thus may limit identity fraud				
Openness	Openness is a meta-FIP that lets various forms of oversight protect all values.							
Access and Correction	MBA	Supports accuracy, and thus fair decisions, or is abused to undercut fairness to others		Threatens security by risking data exposure to identity fraudsters, for example				

Note: Comparing FIPs to the values they may protect shows that most FIPs primarily protect two values: privacy (as control of others' access to information) and fairness. The protection of other values often derives from control, signified by "DC." Some FIPs are potentially antagonistic to some values, undercutting them in certain respects and contexts. This is signified by "MBA," for "may be antagonistic."  
Source: Author.



trust marks are akin to the Underwriters Laboratories certification, which signals to consumers that an electrical device is made to insurers' standards. The TRUSTe seal, one of the most prominent in the past, was meant to show consumers that a website adhered to certain good privacy practices. TRUSTe did not maintain a sterling record itself and settled an action with the FTC in 2014 alleging that it had failed to conduct annual privacy checks of the sites it had certified.<sup>43</sup>

Absent a widely used and recognized trust-mark system, a diffuse welter of mechanisms for market accountability remains, such as news and consumer reporting, competitive attacks among rivals, reputation, and word of mouth (word of tweet). How these influences rank against regulation and litigation is difficult to assess, as market accountability operates so very differently from legal and regulatory accountability.

In any case, yes to accountability. But by saying everything, the accountability FIP risks saying nothing. Other FIPs, such as purpose identification, have more content.

**Purpose Identification.** Purpose identification suggests notifying people in advance about how information about them will be used. Quite simply: privacy policies.

Purpose identification's major service is to position people to refuse an interaction if they do not like anticipated uses of data and other information terms. The *APEC Privacy Framework* said of its notice FIP, "By providing notice, personal information controllers may enable an individual to make a more informed decision about interacting with the organization."<sup>44</sup> Refusing to interact and share data is sharp control of others' access to data. Thus, purpose identification serves access control and thus privacy protection first.

Defense of other values through purpose identification largely derives from access control. In the unlikely event a use will put a person in physical or financial danger, such as a publication likely to reach stalkers or fraudsters, he or she may refuse it. If an identified use is for marketing, similarly, one may reject

interaction because of an interest in peace and quiet, or the more acute interest in integrity against commodification. Some uses may threaten reputation or autonomy and can be refused on that basis.

The theory of purpose identification is not necessarily borne out in practice. In a study of the effects of privacy notices designed to simulate real-world behavior, various privacy-notice types were tested on a representative sample of users.<sup>45</sup> The median amount of time people spent looking at privacy notices before answering survey questions about their sexual behavior ranged from 4.5 to 6.0 seconds—little more than the time it takes to do a quick scan and click through to the next screen.<sup>46</sup> A small minority, 2.3 percent of users, engaged with the material, driving the mean, or average, time spent on the best-quality notice to 19.12 seconds, while the average time spent on a blank screen was 12.59 seconds.<sup>47</sup>

Participants' comprehension of the policies were consistent with the time spent reviewing them. No matter the form of notice, respondents on average answered correctly just one in five questions about the content of a privacy policy.<sup>48</sup> And participants' willingness to share information about risky sexual behaviors deviated little in the study whether they were presented with high- or low-quality privacy notices, or no notice at all. The outlier group that read their privacy policies did not behave differently.<sup>49</sup>

Another study found that consumers think differently, perhaps more intuitively, than the privacy-notice approach assumes. People may rely more on informal norms and trust. When the existence of a privacy policy reminds them that norms may be violated, their trust decreases.<sup>50</sup> Purpose specification may not be consumers' focus when setting boundaries on information collection, retention, sharing, and use.

Purpose specification may have global value, of course. By revealing information practices to advocates, regulators, the press, and politicians, it positions such actors to pressure for different information practices in companies or a given field. This role blends with another FIP discussed below: openness on policies and practices.

Purpose specification can be costly. As is increasingly clear, data can be processed in untold ways to

develop new insights. In commercial contexts, that can produce new efficiencies that reduce costs or improve goods and services, both of which improve consumer welfare. Requiring an organization to commit to certain purposes ahead of time necessarily excludes uses devised later, even though they may be good for everyone. Admitting as much while favoring “pro-social” uses of data, the OECD in 1980 said, “It may be provided that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning.”<sup>51</sup>

This makes purpose identification a conundrum. It positions users to protect privacy and seek fair treatment by declining unwelcome uses, but it requires a commitment to limited uses for all. Thus, it prevents the indifferent from benefiting if information processing would make them better off. This may be why purpose specification in practice includes generalities that permit practically any use in an organization, data sharing with service providers consistent with the organization’s broad purposes, and data sharing with other entities for various legitimate purposes.<sup>52</sup>

Purpose identification is meant to work in tandem with the next FIP, collection with knowledge and consent.

**Collection with Knowledge and Consent.** Knowledge and consent are lynchpins of controlling others’ access to information. When they exist, they are arguably control’s essence. People should know what they are doing when they share information about themselves, and they should articulately decide to do so. The purpose specification FIP discussed above would logically produce knowledge, so that intelligent consent can be exercised. Together, the notice and knowledge and consent FIPs would produce consumer control that means privacy is adequately protected. The theory is strong.

As with purpose identification, privacy through access control is the main value knowledge and consent defend. Protection of other values may derive from controlling others’ access to data. Depending on interest, a person with knowledge may withhold

consent in pursuit of fairness, security, peace and quiet, autonomy, integrity against commodification, and reputation.

Yet, there are acute administrative challenges to the requirement that data should be collected with knowledge and consent. The existence of knowledge is subjective to the person sharing information and not readily accessible to the person collecting it. The latter will have trouble knowing the mindset of the former. As already noted, research suggests that notices do not affect knowledge, as people largely click past them.

---

**Depending on interest, a person with knowledge may withhold consent in pursuit of fairness, security, peace and quiet, autonomy, integrity against commodification, and reputation.**

This FIP also begs the question of what knowledge a person must have. Collection only? Anticipated uses? Risks associated with those uses? Other risks, such as the risks derivative of a data breach? In its discussion of notice and awareness, the FTC said the scope of notice would depend on an entity’s substantive information practices, but “some or all of the following have been recognized as essential”:

- Identification of the entity collecting the data;
- Identification of the uses to which the data will be put;

- Identification of any potential recipients of the data;
- The nature of the data collected and the means by which it is collected if not obvious . . . ;
- Whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
- The steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.<sup>53</sup>

How would an organization of any scale know that the people with whom it interacts are aware of these essential things?

Consent is similarly subjective. Others have to seek clues about the existence and nature of consent. Contract law theory is replete with examinations of what constitutes consent, what demonstrates its existence, and what is consented to.<sup>54</sup> The FIP requiring consent implicates these issues.

Often, knowledge and consent must be assumed and imputed in various ways. In 1980, the OECD called knowledge a “minimum requirement” and said, “Consent cannot always be imposed, for practical reasons.”<sup>55</sup> The FTC combined “choice” with consent, saying, “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.”<sup>56</sup> This vision would require consumers to have a great deal of sophistication and interest in personal information flows.

Efforts to provide choice through granular consent show that it is a challenge. In 2010, the online advertising industry launched the AdChoices program, a self-regulatory effort that allows consumers to opt out of behaviorally targeted advertising. Exercising that option would tend to mollify the interest in integrity against commodification. But a 2016 study found that only 0.23 percent of ad impressions were shown to Americans opting out of behavioral advertising and 0.26 percent of impressions

were shown to people opting out in the European Union.<sup>57</sup> (The number of people opting out cannot be known. Percentage of impressions is a proxy for that number.)

There may be many explanations for this, including difficulty of administering the opt-out and lack of consumer awareness. But the likelihood is that a negligible percentage of consumers are interested in denying advertisers access to information about them for marketing. People would probably overcome the other challenges if opposition to behavioral advertising was something about which a significant number of people felt strongly.

A similar effort to provide granular choice exists in the cookie notices prompted by the EU’s GDPR. Common experience shows they are an obstruction to rapidly click past.<sup>58</sup> Actual knowledge and consent may or may not exist when people click to dismiss such notices, which are meant to educate them about information policies.

Knowledge and consent are excellent ideals that are challenging to administer. The next FIP, limited collection, does not require knowing the minds of others, but it poses different challenges.

**Limited Collection to Where Necessary for Purpose.** Online interactions create a lot of data and opportunities to collect personal data. Data storage is inexpensive, and a default in most institutions is to keep data for a long time.<sup>59</sup> That is easy to treat as a problem—though precisely what problem is important to consider. The FIP calling for limited collection of personal information addresses the problem by instilling an ethic of limiting collection to necessity.

Only data necessary to the purposes of an interaction should be collected, according to this FIP. That rule supports access control and thus privacy because it causes service providers to cabin their data collection even if consumers do not control their sharing. Secondly, it protects many other values, because tightly circumscribed data collection will block data sharing and many forms of misuse. For example, collection limitation may enhance security, both personal and financial, because to some small degree it

may reduce data availability to wrongdoers. Limiting collection to what is necessary may gratify people interested in integrity against commodification because it will constrain corporate access to personal data. These are highly contextual and sometimes fairly thin benefits.

Collection limitation may undermine the protection of other values, though also narrowly. Without good information about people, marketing messages are more likely to be misdirected. People interested in peace and quiet or integrity against commodification may end up slightly worse off for receiving errant marketing messages. More information may help secure against identity fraud or preserve or restore reputations. Again, on narrow margins.

This FIP raises interesting and challenging questions, too, including where the “necessity” line should be drawn. It is not easy to balance the sensitivity of information against its utility and decide which unit of data collection is too much. Commentary on the APEC collection limitation principle treats the purpose of collection as a touchstone and says, “Proportionality to the fulfillment of such purposes may be a factor in determining what is relevant.”<sup>60</sup> It is thoughtful language, but it does not establish any meaningful standard. Like many of its peers, the limited collection FIP is somewhat question-begging, a challenge that manifests itself through the FIP requiring adherence to use limitations, discussed below.

It also biases against data collection that might serve consumers’ overall interests. If people are indifferent to whether information is shared, or if they wish to share information liberally to benefit from processing, this FIP actually cuts against their wishes and well-being. They may end up with privacy they do not want.

The limited collection FIP deviates from the consumer-choice premise of others. Indeed, the FIPs vacillate between choice and prescription. The next FIP Bennett and Raab identified returns to embracing choice.

**Limited Use and Disclosure.** A natural adjunct to the first two FIPs above, purpose identification and sharing with knowledge and consent, is

limiting use and disclosure to the terms specified in privacy policies. Free to do what they say they will do, data controllers should refrain from doing what they say they will not do. The HEW report recommended having “a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.”<sup>61</sup>

This FIP positions those who have benefited from purpose identification and knowing consent (or refusal) to get the use limitations they expect. Three FIPs serving one value: control. Limits on use and disclosure may also protect security, peace and quiet, and other values, depending on circumstances.

A challenge arises in limiting use and disclosure according to the purposes of collection, and that is determining what exactly the purposes of collection are. They may be subject to vastly different interpretations. The EU data protection directive’s working party confessed this problem when it wrote in 1998 that data, once processed, should be used or communicated “insofar as this is not incompatible with the purpose of the transfer.”<sup>62</sup> That concession, from purpose to compatibility, still leaves a lot to interpretation. Without knowing precisely what the original purposes are, it is hard to know what is compatible with them.

Consistent with consumer choice, the limited use principle allows limits on use to be changed. This is an outgrowth of purpose identification and collection with knowledge and consent. People can change their minds post-collection to meet their full preferences. The next FIP, though, oscillates back away from the consumer-choice model.

**Retention Only as Long as Necessary.** Because data that exist can be shared, data retention affects control of others’ access to information along the time dimension. Limiting retention reduces the availability of personal information to sharing and use, so it decreases the likelihoods of lost control and exposure through data breach and policy violation, for example. The FIP that circumscribes data retention serves access control and thus privacy by reducing those risks.



To a lesser but still relevant extent, limiting retention can reduce the invasiveness of data collection and marketing behavior that offend integrity against commodification. Retained data can threaten autonomy, which is the interest in acting free of social and legal repercussions. Because being wrongly judged in social settings is so offensive, many gravitate toward perceiving data retention as threatening reputation, but retained data can be used equally to build reputations.

Therefore, limiting data retention is not an unalloyed good. Having more data available for decision-making will, over time and in aggregate, probably tend to improve fairness. And in some applications, data retention improves things for people, such as when retained data can frustrate identity fraud. Limiting retention could increase such fraud by some small margin.

The limited retention principle shares the quality of prescriptiveness with the limited collection principle. This means people who are indifferent or prefer data retention are unlikely to get it. That could leave them worse off on some margins, because deeper stores of information about them are not available to processors. The next FIP is meant to ensure that consumers are better off in terms of fairness, if not privacy as control.

**Data Kept Accurate, Complete, and Up-to-Date (Data Quality).** The HEW report said that organizations “must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.”<sup>63</sup> Data should be “up to” whatever the decision-making task. Misuse, it might be inferred, is using data in unsupportable ways. This is to get people their due when organizations make decisions about them.

Data quality is a natural part of fairness. Inaccurate data may produce inaccurate results that treat individuals wrongly. It is a simple logic. That logic applies equally to the interest in reputation, in which wrong information may result in unfair social determinations. Inaccuracy goes into the anti-commercial sensibility at the heart of integrity against commodification too. Big companies can do a lot of damage with mechanistic and unfair decisions.

While having accurate data helps ensure fairness directly, accuracy conflicts with controlling others’ access to information and thus privacy. Having inaccurate information in a dataset fosters access control in a unique way because the data holder knows less about the data subject, even if it thinks it knows more. Indeed, if information is inaccurate in the right respects, it may no longer be true personal information, even though it appears to be. It is just information that purports (wrongly) to be about a person.

---

**Because being wrongly judged in social settings is so offensive, many gravitate toward perceiving data retention as threatening reputation, but retained data can be used equally to build reputations.**

Imagine that a marketer has address information associated with your name that is 20 years out-of-date. You have moved six times since it was correct. Yet envelopes keep arriving where you once lived, inviting you to buy the mattress that can truly solve your sleep issues or the cleaning products that can make your oven truly sparkle. But in your yurt far away, you sleep on a mat after cooking dinner over a coal fire.

The mailings are a minor invasion of peace and quiet for the people who live there now—and perhaps their commercial sensibilities. They must toss out mis-addressed mail occasionally. Nothing is really happening to you, though, when data about you are inaccurate. You are missing offers that would not intrigue you.

Something is happening to the data holder: It is failing to reach the person it thinks it is reaching and probably losing a small amount of money for the effort. That is nobody's problem but its own. Correcting the data would make it your problem, as your peace and quiet might then suffer compromise. And when you experience the badly misdirected content of the ads, you might adopt a loathing of crass commercialism.

It feels important to have data about oneself be accurate, but in many or most data banks, it may not be important at all. Let them have their wrong information. That provides a margin of information control to the data subject.

It is fascinating that pushing for accuracy, a prominent tenet of what people consider "privacy" practices, is at odds with one of privacy's most central senses. Accuracy's aim for fairness may come at the expense of controlling others' access to information. The next FIP, security, seems more consistently and broadly important.

**Security Safeguards.** Security is important for reasons wholly separate from privacy and related values. Organizations that do not secure their assets and processes may lose the capacity to produce, make decisions, communicate, retain employees, and collect revenues. They cannot carry out their promises, whether to deliver goods and services or deliver on privacy or other data protections.

Security safeguards are an important adjunct to data retention and disclosure policies because such policies are reliable only when the promisor can fulfill them. Security protects controlled sharing of information. To a smaller degree, security is an adjunct to fairness, as corrupted or altered data may result in wrong or unfair decisions. Finally, security safeguards have a clear nexus with financial security, as they prevent the release of important tools for theft or financial fraud. There may be a minor connection to personal security, too, as security of information keeps one from being a target of personal attack and from the attack being carried out.

The expression Bennett and Raab give to the security FIP calls for "appropriate security safeguards."<sup>64</sup> This is as question-begging as many of the

other FIPs, which are somewhat plagued by open meanings. Most of the meaning is in the pregnant word "appropriate."

As with accountability, yes to security. Exactly what that means is highly contextual, as are many FIPs, including the next one, openness.

**Openness on Policies and Practices.** Although they seem similar because both provide information to the public, the openness FIP is distinguishable from the purpose identification FIP, which roughly summarizes to "privacy policies." While privacy policies refer to discreet information practices and policies, openness appears to promote transparency of operations.

Openness has excellent provenance. The HEW report's first recommendation was: "There must be no personal data record-keeping systems whose very existence is secret."<sup>65</sup> (That is a starting point on openness, at least.) The report's recommendation for legislation modeled on fair labor practices suggests that collective action to protect consumers may have been in the authors' collective mind. Ware was conscious of power, saying in his summary of the HEW report, "The preferred solution would adjust the balance of power between citizen and record system."<sup>66</sup> Openness empowers overseers, including those on panels such as the one Ware chaired.

Openness is a meta-FIP like accountability. Indeed, openness is a means to accountability. Its purpose according to the OECD is to facilitate administration of other FIPs, such as access and correction, as discussed below. When seeking to exercise such rights, "Individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost."<sup>67</sup>

Designing open or transparent social systems is a challenge. It is a two-sided problem, as there must be sufficient information or data expressed in a suitable way and there must also be a community motivated to digest the information.<sup>68</sup> The AdChoice program discussed above may lack either factor, or both. The next FIP, access and correction, also requires a motivated community if it is to have effects.

**Access and Correction.** The data quality FIP discussed above imposed a responsibility on decision makers to use good data. The access and correction FIP invites data subjects into that conversation.

“There must be a way for an individual to find out what information about him is in a record and how it is used,” recommended the HEW report.<sup>69</sup> The expert group that produced the OECD report in 1980 called it “the most important privacy protection safeguard.”<sup>70</sup>

The precise value access and correction probably protect is not privacy, but fairness. A person accessing and then correcting personal information can help ensure that data-using decision makers render more accurate decisions.

The access and correction FIP creates interesting tensions. One is the tension with security. Any system that opens up access to customarily closed data may expose information about data subjects to impostors. Someone who knows what identifiers a person has used may impersonate them on the system and collect more information about them, perhaps using it to attack them or gain access to more data in other systems. Granting more access increases a data system’s “attack surface.” Thus, access and correction threatens control of others’ access to information, as well as personal and financial security, for example. The APEC privacy principles acknowledged this, recognizing the need for proof of identity before providing access and suggesting that security requirements may preclude “direct access” to information.<sup>71</sup>

Giving people the power to correct information about themselves in databases may conflict with control over others’ access to information in another way. If people do as expected and increase the accuracy of information about themselves in databases, slightly more information will reside in the hands of others. Conversely, correction rights may increase control by allowing people to falsify information about themselves and thus make themselves more obscure.

Correction rights may conflict with fairness if used “dishonestly.” If people use correction rights to erase true but derogatory information or to create false complimentary information, that will cause them to be treated better than they should be. When

goods are allocated from a fixed or static pie, such as elite college admissions, that would necessarily imply poorer treatment of others.

The APEC privacy principles also recognized certain competitive challenges that access rights may create. Personal data may be inextricably intertwined with data structures or processing techniques. Providing access to that data may reveal proprietary business information and methods. According to APEC, “Organizations may deny or limit access to the extent that it is not practicable to separate the personal information from the confidential commercial information.”<sup>72</sup> This final FIP Bennett and Raab listed has a complex relationship with privacy and related values.

Ultimately, FIPs are accurately named. They have been motivated as much by the idea of securing fair treatment for people as protecting their privacy by giving them control over others’ access to information. Summarizing the full HEW committee report in August 1973, Ware emphasized the uses institutions made of data as opposed to gathering or disclosure.

Relative to the totality of the record-keeping systems that surround each of us today, any one individual finds himself at a significant disadvantage to affect the content of the records or to limit their usage. Most of us have suffered at least the annoyance of having to cope with a computer-based system that, outwardly at least, appears not to care how it has mistreated us or, worse, has given false impression or subjected us to harassment.<sup>73</sup>

Ware was more concerned with Franz Kafka than George Orwell. The FIPs that developed from the HEW report and other early explorations reflect similar motivations. Receiving good treatment seems as important as controlling others’ access to personal data.

The integrity against commodification value gets top treatment among secondary interests protected by FIPs. The bias of some FIPs against collection and retention, even when other FIPs allow those matters to be negotiated, seems designed to satisfy anti-commercial concerns.

Many other values receive scant attention from FIPs. People have extensive interests beyond controlling information about themselves and receiving fair treatment. The many interests that are derivative of control—personal and financial security, autonomy, and so on—could be protected directly.

To the extent they are considered “principles,” FIPs do not provide a vision of data protection that spans the threatened interests people have. As “practices,” FIPs do not provide enough clarity and precision to guide action. In the end, what the FIPs “do” is not so much protect consumers as pose questions about how to protect consumers.

### FIPs as a Rolling Inquiry

Part of FIPs’ attraction for experts may be that they create a set of complex questions to pore over in the name of privacy and data protection. FIPs-based regulation and compliance create a tremendous amount of work and cost that may not concretely and directly address people’s true priorities and problems. FIPs are not answers but an invitation to a rolling inquiry that continues 50 years along.

The EU’s General Data Protection Regulation (GDPR) is the latest and most important in the FIPs line. One might expect it to reveal how FIPs apply in concrete terms, and it did give a few paragraphs each to many of the FIPs in its 88 pages of finely printed text. (It has 173 “whereas” clauses and 11 chapters containing 99 articles of regulatory planning text.) The GDPR includes special rules pertaining to children and the processing of special categories of personal data. It created a new “right to be forgotten” by having data erased.<sup>74</sup>

Much of the GDPR, though, is dedicated to administration: It imposes a new responsibility on data controllers to conduct “data protection impact assessments.”<sup>75</sup> It details jurisdictional matters; creation and functioning of supervisory authorities in EU member states; cooperation among supervisory authorities; the creation of a European Data Protection Board to promote consistency among supervisory authorities; requirements on controllers and

processors to have data protection officers; codes of conduct to be established by associations representing controllers or processors; certification bodies, seals, and marks; administration of data transfers to non-EU countries; and so on. The European Data Protection Board has issued dozens of opinions, notices, and letters covering nearly 100 topics since its formation in 2018.<sup>76</sup>

---

## FIPs are not answers but an invitation to a rolling inquiry that continues 50 years along.

Repealing the 1995 European Union’s data protection directive, GDPR began a second rolling inquiry across a multi-jurisdictional regulatory network about how institutions should behave with respect to personal information. Any actor working with personal information affecting Europeans must monitor this regulatory network to know right from wrong in personal data collection and use. Right and wrong under GDPR is *malum prohibitum*—legal Latin for things that are wrong because they are banned. They are not *malum in se*—things that are wrong in and of themselves. The GDPR’s requirements and proscriptions are not intuitive, certainly not to privacy laypeople.

There are alternatives to FIPs-based privacy regulation and protection. For example, the questions could be framed around the four major activities that data controllers participate in: collection, retention, sharing, and use. Each has distinct consequences.<sup>77</sup>

There is yet another way to approach privacy and data protection, which was exhibited when the Working Party on the Protection of Individuals with regard to the Processing of Personal Data included special provisions in its work on data flows to third countries. These special provisions remarkably correlate to the values I identified in my study of the values affected by information technology.<sup>78</sup> The working group



included a special provision for data transfers for direct marketing purposes, for example, saying these should be subject to opt out at any stage.<sup>79</sup> This pursues integrity from commodification.

The working group also identified certain categories of transfer that pose particular risks, including “transfers which carry the risk of financial loss” (financial security), “transfers carrying a risk to personal safety” (personal security), “transfers made for the purpose of making a decision which significantly affects the individual” (fairness), “transfers which carry a risk of serious embarrassment or tarnishing of an individual’s reputation” (reputation), and “transfers which may result in specific actions which constitute a significant intrusion into an individual’s private life, such as unsolicited telephone calls” (peace and quiet).<sup>80</sup> Thus, human values have crept organically into a process that was set up as a logical exercise.

Focusing on protecting human values might produce rules that are more intuitive, more administrable, and thus better. The deductive methods epitomized by FIPs, and the administration they require, can be enervating. With a 50-year history and a practitioner community steeped in FIPs’ orthodoxies, though, it may take some doing to upgrade from FIPs to a better methodology.

## Conclusion

When he suggested a notice regime at the September 1972 meeting of the Secretary’s Advisory Committee on Automated Personal Data Systems, one of the responses Willis Ware received was from Charles Borsom, executive vice president of the National Society of Comptrollers and Financial Officers. Borsom said:

When the public comes to a lender and says, lend me some money; they are a lot more interested in how much it is going to cost, when they are going to get it, how they have to pay it back, what happens if they don’t pay it back, than they are about whether the personal information they give is going to go to any other credit bureau.<sup>81</sup>

Borsom believed a special notice would not receive much attention, suggesting that the goal of inspiring people to privacy self-protection would flounder. He may have been right.

## Human values have crept organically into a process that was set up as a logical exercise.

Things might be different if privacy and information policy were grounded not in high-level principles or practices but in the values people hold dear. What should be done to give people desired control of others’ access to information about them? What makes for fair institutional decision-making processes? What is the best way to protect people and assure them of their financial and personal security? What allows people to be left alone as they wish, whether the preference is animated by simple peace or antipathy to commercialism? What data collection and storage should be resisted to protect people’s autonomy from overweening social and legal constraints? And what allows good behavior to engender good reputations for people, while bad behavior justifiably makes people look bad?

FIPs are a complex, involved inquiry into what organizations should do. They do not seem to protect this suite of important values directly or clearly. Although produced by thoughtful people with good intentions, they do not have the spark of life that comes from the important prospect of protecting people from harm and making their lives better overall.

In 50 years, FIPs have not met the challenge of Information Age data uses that still rush over our society. FIPs-based legislation has not solved the privacy problem and cannot be expected to, certainly not in one fell swoop. Other modes for responding to Information Age challenges may be better suited to protecting privacy and related values.

**About the Author**

**Jim Harper** is a visiting fellow at the American Enterprise Institute, where he focuses on privacy issues and select legal and constitutional law issues.

# Notes

1. See Meir Kohn, “Trading Costs, the Expansion of Trade and Economic Growth in Pre-Industrial Europe” (working paper, Dartmouth College, Hanover, NH, January 8, 2001), <https://cpb-us-e1.wpmucdn.com/sites.dartmouth.edu/dist/6/1163/files/2017/03/00-05.pdf>.
2. In medieval times, ordinary possessions were “not esteemed of so high a nature, nor paid so much regard to by the law, as things that are in their nature more permanent and *immoveable*, as land and houses, and the profits issuing thereout.” Travel and commerce necessitated putting personality “in a light nearly, if not quite, equal to . . . realty.” William Blackstone, *Commentaries on the Law of England in Four Books*, vol. I (1765; Philadelphia, PA: J. B. Lippincott Co., 1893). Richard Pipes states, “Sometime during the period in European history vaguely labeled ‘early modern,’ there occurred a major break in the attitude toward property. It was the consequence of the remarkable expansion of commerce which began in the late Middle Ages and accelerated following the discovery of the New World.” Richard Pipes, *Property and Freedom* (New York: Alfred A. Knopf, 1999), 25. Eric Jones examines theories that might explain how personal property rights took hold. Eric Jones, *The European Miracle: Environments, Economies and Geopolitics in the History of Europe and Asia*, 3rd. ed. (Cambridge, UK: Cambridge University Press, 2003).
3. See Jonathan Rauch, “The Constitution of Knowledge,” *National Affairs* 37 (Fall 2018), <https://www.nationalaffairs.com/publications/detail/the-constitution-of-knowledge>.
4. See Stijn Broecke and Sandrine Cazes, “The Platform Economy Can Deliver for Its Workers Too,” *OECD Observer*, June 2019, [https://oecdobserver.org/news/fullstory.php/aid/6223/The\\_platform\\_economy\\_can\\_deliver\\_for\\_its\\_workers\\_too.html](https://oecdobserver.org/news/fullstory.php/aid/6223/The_platform_economy_can_deliver_for_its_workers_too.html).
5. W. H. Ware, *Future Computer Technology and Its Impact*, RAND Corporation, March 1966, <https://www.rand.org/content/dam/rand/pubs/papers/2008/P3279.pdf>.
6. Willis Ware contacted me in the 2000s—in his 80s—for a short correspondence that I take as evidence of his abiding curiosity and sincere interest in privacy.
7. See Jim Harper, *Privacy and the Four Categories of Information Technology*, American Enterprise Institute, May 26, 2020, <https://www.aei.org/research-products/report/privacy-and-the-four-categories-of-information-technology/>.
8. US Department of Health, Education, and Welfare, Office of the Secretary, Secretary’s Advisory Committee on Automated Personal Data Systems, transcript of proceedings, September 29, 1972, 220–21, [https://www.law.berkeley.edu/files/HEW/HEW\\_transcript\\_09291972.pdf](https://www.law.berkeley.edu/files/HEW/HEW_transcript_09291972.pdf).
9. US Department of Health, Education, and Welfare, Office of the Secretary, Secretary’s Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, July 1973, xxiii, <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>.
10. US Department of Health, Education, and Welfare, Office of the Secretary, Secretary’s Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, xx–xxi.
11. The Kenneth Younger report’s principles are: “(1) Information should be regarded as held for a specific purpose and not to be used, without appropriate authorization, for other purposes. (2) Access to information should be confined to those authorized to have it for the purpose for which it was supplied. (3) The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose. (4) In computerised systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data. (5) There should be arrangements whereby the subject could be told about the information held concerning him. (6) The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information. (7) A monitoring system should be provided to facilitate the detection of any violation of the security system. (8) In the design of information systems, periods should be specified beyond which the information should not be retained. (9) Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information. (10) Care should be taken in coding value judgments.” This quotation can be found at Robert Gellman, “Fair

Information Practices: A Basic History” (unpublished manuscript, January 26, 2021), 5–6, <https://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.

12. Privacy Act of 1974, 5 USC § 552a (1974).

13. As identified by the Privacy Protection Study Commission, the eight principles animating the Privacy Act were: “(1) There shall be no personal-data record-keeping system whose very existence is secret and there shall be a policy of openness about an organization’s personal-data record-keeping policies, practices, and systems. (The Openness Principle) (2) An individual about whom information is maintained by a record-keeping organization in individually identifiable form shall have a right to see and copy that information. (The Individual Access Principle) (3) An individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information. (The Individual Participation Principle) (4) There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information. (The Collection Limitation Principle) (5) There shall be limits on the internal uses of information about an individual within a record-keeping organization. (The Use Limitation Principle) (6) There shall be limits on the external disclosures of information about an individual a record-keeping organization may make. (The Disclosure Limitation Principle) (7) A record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate. (The Information Management Principle) (8) A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems. (The Accountability Principle).” See Privacy Protection Study Commission, *Personal Privacy in an Information Society*, July 1977, 501–2.

14. The first national legislation aimed at protecting privacy, Sweden’s 1973 Data Act, did not contain data protection principles. It required processors of personal data to get a permit from a new data protection authority, the Data Inspection Board, which would issue tailor-made conditions for each personal information processor. See Sören Öman, “Implementing Data Protection in Law,” in *Scandinavian Studies in Law: IT Law*, vol. 47, ed. Peter Wahlgren (Stockholm, Sweden: Stockholm Institute for Scandinavian Law, 2004), 390, <http://www.sorenoman.se/Implementing.pdf>.

15. Robert Gellman, “Fair Information Practices: A Basic History” (unpublished manuscript, October 7, 2019), 2–4, <https://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.

16. See, for example, International Association of Privacy Professionals, “Fair Information Practice Principles,” <https://iapp.org/resources/article/fair-information-practices/>.

17. Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: MIT Press, 2006), 4.

18. Bennett and Raab, *The Governance of Privacy*, 10.

19. Bennett and Raab, *The Governance of Privacy*, 10.

20. Oren Bar-Gill, Omri Ben-Shahar, and Florencia Marotta-Wurgler, “Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts,” *University of Chicago Law Review* 84, no. 1 (Winter 2017): 7–35, <https://chicagounbound.uchicago.edu/uclev/vol84/iss1/2/>. But see Gregory Klass, “Empiricism and Privacy Policies in the Restatement of Consumer Contract Law,” *Yale Journal on Regulation* 36, no. 1 (Winter 2019): 45–115, <https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3005&context=facpub>. US Supreme Court Justice Neil Gorsuch argued that those contracts create bailments, a property law concept. *Carpenter v. United States*, 585 US \_\_\_, 2268–69 (2018).

21. Bennett and Raab, *The Governance of Privacy*, 9.

22. Fred H. Cate, “The Failure of Fair Information Practice Principles,” in *Consumer Protection in the Age of the ‘Information Economy’*, ed. Jane K. Winn (Burlington, VT: Ashgate, 2006), 346.

23. Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980, <http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protection of privacy and transborder flows of personal data.htm>. The Organisation for Economic Co-operation and Development’s principles were: “(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. (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.” See Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

24. Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

25. Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (working document, European Commission, Brussels, Belgium, July 24, 1998).

26. European Parliament and Council of the EU, Directive 95/46/EC, October 24, 1995, in *Official Journal of the European Union*, L 281 (November 23, 1995), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>.

27. Those principles were: “(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. . . . (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 organisational security measures should be taken by the data controller that are appropriate to the risks presented by the 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. . . . Examples of additional principles to be applied to specific types of processing are: (1) Sensitive data—where ‘sensitive’ categories of data are involved [racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion, health, or sexual life], additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing. (2) Direct marketing—where 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. (3) 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." See Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Transfers of Personal Data to Third Countries*.

28. European Parliament and Council of the EU, Directive 95/46/EC.

29. Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998, <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>.

30. Federal Trade Commission, *Privacy Online: A Report to Congress*. Compare it with Colin J. Bennett and Charles D. Raab: "Unless customers or citizens can trust others with their personal details or their political opinions, so goes the argument, governmental efficiency, economic prosperity, and the renewal of democratic practices and institutions will suffer." Bennett and Raab, *The Governance of Privacy*, 51.

31. Children's Online Privacy Protection Act of 1998, 15 USC §§ 6501–6506 (1998).

32. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, May 2000, <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>.

33. The Asia-Pacific Economic Cooperation privacy principles are: (1) Preventing harm—"Personal information protection should be designed to prevent the misuse of such 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." (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." (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." See Asia-Pacific Economic Cooperation Secretariat, *APEC Privacy Framework*, December 2005, <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework>.

34. Asia-Pacific Economic Cooperation Secretariat, *APEC Privacy Framework*.

35. European Parliament and Council of the EU, Regulation (EU) No. 2016/679, April 26, 2016, in *Official Journal of the European Union*, L 119/1 (May 4, 2016), <https://gdpr-info.eu/art-5-gdpr/>.

36. See Ken Nguyen, "Comparison: California Consumer Privacy Act and Fair Information Practice Principles," Medium, December 22, 2019, [https://medium.com/@ken\\_nguyen/comparison-california-consumer-privacy-act-and-fair-information-practice-principles-f72e08204807](https://medium.com/@ken_nguyen/comparison-california-consumer-privacy-act-and-fair-information-practice-principles-f72e08204807).

37. Woodrow Hartzog, “The Inadequate, Invaluable Fair Information Practices,” *Maryland Law Review* 76, no. 4 (2017): 952–83, <https://digitalcommons.law.umaryland.edu/mlr/vol76/iss4/4/>.
38. Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.
39. See Harper, *Privacy and the Four Categories of Information Technology*.
40. Bennett and Raab, *The Governance of Privacy*, 12–13.
41. Federal Trade Commission, *Privacy Online: A Report to Congress*.
42. Florencia Marotta-Wurgler, “Self-Regulation and Competition in Privacy Policies,” *Journal of Legal Studies* 45, no. S2 (June 2016): S13–39, <https://www.journals.uchicago.edu/doi/10.1086/689753>.
43. Federal Trade Commission, “TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program,” press release, November 17, 2014, <https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its>.
44. Asia-Pacific Economic Cooperation Secretariat, *APEC Privacy Framework*.
45. Omri Ben-Shahar and Adam Chilton, “Simplification of Privacy Disclosures: An Experimental Test,” *Journal of Legal Studies* 45, no. S2 (June 2016): S41–67, <https://www.journals.uchicago.edu/doi/10.1086/688405>.
46. Ben-Shahar and Chilton, “Simplification of Privacy Disclosures.”
47. Ben-Shahar and Chilton, “Simplification of Privacy Disclosures.”
48. Ben-Shahar and Chilton, “Simplification of Privacy Disclosures.”
49. Ben-Shahar and Chilton, “Simplification of Privacy Disclosures.”
50. Kirsten Martin, “Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online,” *Journal of Legal Studies* 45, no. S2 (June 2016): S191–215, <https://www.journals.uchicago.edu/doi/10.1086/688488>.
51. Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.
52. Joel R. Reidenberg et al. state: “The causes of vagueness may be due to a desire for flexibility, or it may be due to the policy author’s incomplete knowledge about the actual data practices.” Joel R. Reidenberg et al., “Ambiguity in Privacy Policies and the Impact of Regulation,” *Journal of Legal Studies* 45, no. S2 (June 2016): S163–90, <https://www.journals.uchicago.edu/doi/10.1086/688669>.
53. Federal Trade Commission, *Privacy Online: A Report to Congress*.
54. For example, Randy E. Barnett states, “What exact meaning must a court conclude was conveyed by a promisor to a promisee to find that a contractual commitment was incurred? If consent is properly thought of as ‘objective’ or ‘manifested’ assent, what is it that must be assented to for a contractual obligation to arise?” Randy E. Barnett, “A Consent Theory of Contract,” *Columbia Law Review* 86 (1986): 269–321.
55. Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.
56. Federal Trade Commission, *Privacy Online: A Report to Congress*.
57. Garrett A. Johnson, Scott K. Shriver, and Shaoyin Du, “Consumer Privacy Choice in Online Advertising: Who Optes Out and at What Cost to Industry?” (working paper, University of Rochester, Simon Business School, Rochester, NY, June 19, 2019), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3020503](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3020503).
58. Matt Burgess writes, “GDPR’s implementation fundamentally changed the experience of using the web in another, more annoying, way: popups.” Matt Burgess, “The Tyranny of GDPR Popups and the Websites Failing to Adapt,” *Wired*, August 29, 2018, <https://www.wired.co.uk/article/gdpr-cookies-eprivacy-regulation-popups>.
59. See Harper, *Privacy and the Four Categories of Information Technology*.
60. Asia-Pacific Economic Cooperation Secretariat, *APEC Privacy Framework*.
61. US Department of Health, Education, and Welfare, Office of the Secretary, Secretary’s Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, xx–xxi.

62. Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Transfers of Personal Data to Third Countries*.
63. US Department of Health, Education, and Welfare, Office of the Secretary, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, xxi.
64. Bennett and Raab, *The Governance of Privacy*, 12.
65. US Department of Health, Education, and Welfare, Office of the Secretary, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, xx.
66. Willis H. Ware, *Records, Computers and the Rights of Citizens*, RAND Corporation, August 1973, <https://www.rand.org/pubs/papers/P5077.html>.
67. Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.
68. See Jim Harper, "Publication Practices for Transparent Government," Cato Institute, September 23, 2011, <https://www.cato.org/publications/briefing-paper/publication-practices-transparent-government>.
69. US Department of Health, Education, and Welfare, Office of the Secretary, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, xx.
70. Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.
71. Asia-Pacific Economic Cooperation Secretariat, *APEC Privacy Framework*.
72. Asia-Pacific Economic Cooperation Secretariat, *APEC Privacy Framework*.
73. Ware, *Records, Computers and the Rights of Citizens*.
74. European Parliament and Council of the EU, Regulation (EU) No. 2016/679.
75. European Parliament and Council of the EU, Regulation (EU) No. 2016/679.
76. See European Data Protection Board, "Our Documents," [https://edpb.europa.eu/our-work-tools/our-documents\\_en](https://edpb.europa.eu/our-work-tools/our-documents_en).
77. See Harper, *Privacy and the Four Categories of Information Technology*.
78. See Harper, *Privacy and the Four Categories of Information Technology*.
79. Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Transfers of Personal Data to Third Countries*.
80. Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Transfers of Personal Data to Third Countries*.
81. US Department of Health, Education, and Welfare, Office of the Secretary, Secretary's Advisory Committee on Automated Personal Data Systems, transcript of proceedings, 226.