Introduction

Information privacy law in the United States is currently a bewildering assortment of many types of law that differ from state to state and in federal statutes and regulations. Information privacy law concerns the collection, use, and disclosure of personal information. At present, it is unwieldy and conflicting. There is another result of American information privacy law's current status as a cacophony of so many different laws and regulations. The state of this area of U.S. law has led many foreign nations to discount the protections that do exist here. The EU, for example, has little respect for U.S. information privacy law, and its view of U.S. law is creating significant tensions and problems for smooth transborder data flows and efficient commerce between EU members and the United States.

Information privacy law is, therefore, an area of law that requires the type of guidance that the ALI can bring. This draft is organized around key Fair Information Practice Principles (FIPPs). FIPPs are a set of principles about the responsibilities that entities should have when collecting and using personal data. They also provide the rights that people should have regarding their data. The initial set of FIPPs were originally articulated in 1973, and have subsequently been restated and expanded a number of times. Despite this revisiting, FIPPs have remained essentially the same during the past 40 years. They have also been extremely influential. FIPPs form the backbone of privacy law in the United States and around the world.

FIPPs are already the foundation of much privacy law, and, as a consequence, they represent the best place to focus the ALI project. FIPPs need to be restated; they need more flesh on the bone; they need to provide sufficient guidance to bring uniformity and clarity to the law. FIPPs have been articulated many times, but each articulation has been incomplete and has not contained sufficient detail and guidance to make FIPPs more useful. Moreover, FIPPs have not been adequately harmonized with the common law. New legal principles that have developed are not sufficiently included in these principles. This draft is designed to develop and advance FIPPs into a set of principles that will provide the kind of guidance that information privacy law needs.
Questions and Comments for the Advisers and the Members Consultative Group

1. We have chosen to use the approach to personally identifiable information (PII) that we have proposed in one of our articles—to have full protections for identified data and only some, but not all, protections for identifiable data. Are there alternative approaches that are practical and viable?

2. What is adequate notice? How specific should privacy notices be? As former FTC Chairman Jon Leibowitz stated, “Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don’t notice, read, or understand the privacy policies.” How are these problems to be addressed?

3. In § 5 (Consent), we include a provision about using “only the minimum necessary information to achieve the purpose for the use, collection, or disclosure.” Should additional guidance and more concrete language be used here?

4. Throughout § 5, the concept of “reasonableness” is used quite substantially. We wanted this provision to have sufficient flexibility and not be too rigid or constraining. Is there a better way to achieve flexibility yet also provide meaningful guidance about this challenging issue?

5. We include § 6 (Confidentiality), which oddly is not codified explicitly in many versions of the FIPPs. It is clearly implied, but often not spelled out. The common law is much more developed when it comes to confidentiality and its exceptions, so we looked to the common law to craft this provision.

6. We include § 8 (Purpose Limitation), one of the more contested of the FIPPs. The principle of purpose limitation was drafted purposefully to be quite vague. Could it use some additional fleshing out? One concern is that the provision as drafted does not specify what “relevance” is, how this is to be determined, or the consequences for using data in ways that are not relevant. How would we develop this without making the principle too restrictive or contested?

7. In § 9 (Use and Disclosure Limitation), we directly prohibit uses that intentionally or negligently cause harm to individuals. We fuse common law with FIPPs for the concepts in this provision. Should we flesh out more how to define “harm”? And what additional guidance can be provided about what constitutes negligence in the context of the use of personal data?

8. In § 12 (Destruction of Data), we include a milder form of the “right to be forgotten,” an idea which is now discussed in the EU. The “right to be forgotten” itself is poorly named because rarely is all of a person’s data 100 percent forgotten. Instead, the debate concerns reasonable restrictions on data retention. There are countless U.S. laws that regulate data retention. We have sought to generalize from these laws. Are there exceptions beyond those we list? We also have a data disgorgement provision for data obtained in violation of the Information Privacy Principles.

---

1 So Private, So Public: Individuals, the Internet & the Dilemma of Behavioral Marketing, FTC (Jon Leibowitz, Town Hall Meeting on Behavioral Advertising: Tracking, Targeting, & Technology), 2007 WL 3352514 (Nov. 1, 2007).
Are there any legitimate reasons why data obtained in violation of the Information Privacy Principles should ever be retained?

9. Regarding § 13 (Portability of Data), we would like input on the validity of this concept. Should we include this principle on data portability?

10. The principle § 16 (Redress for Harm) is one of the more complex and controversial issues we need to address. How should harm be defined? The law has struggled significantly with the issue of what constitutes harm when data is misused. In many cases, privacy harms can be small. For example, consider a notice that could have been clearer and that resulted in the use of data for a marketing campaign to people. Imagine that some people were annoyed by the unexpected marketing, but that they are unable to point to a significant harm. How should we provide appropriate redress for such violations that creates the optimal deterrence without overly penalizing the wrongdoer? A small amount of harm (such as $1 per individual) can add up in the data privacy context when data is gathered about millions (sometimes billions) of people. We included subsection 4 to allow courts to craft other forms of redress. Are there other approaches or solutions?

11. Are there any principles we should also be including?