4-8-2019

Reporters' Memorandum

Paul M. Schwartz
Berkeley Law

Daniel J. Solove

REPORTERS' MEMORANDUM

Principles of the Law, Data Privacy

Paul M. Schwartz
Jefferson E. Peyser Professor of Law
UC Berkeley School of Law

Daniel J. Solove
John Marshall Harlan Research Professor of Law,
George Washington University Law School

April 8, 2019

For the 2019 Annual Meeting, we are delighted to present our entire Principles of the Law, Data Privacy. The Council has approved all the Principles, and we will now present the draft to the members.

Background

At the Fall 2016 Council meeting in New York, the first three Principles were approved. The Council also offered suggestions for revisions and tweaks for us to consider, and we took these into account in making changes to those three Principles. We then submitted Principles §§ 4-10 to the Council at its October 2017 meeting in New York. At this meeting, the Council approved §§ 6, 7, and 8. It decided to hold over its consideration of §§ 4 and 5 and discuss them at the same time as the Section devoted to "Enforcement."

On November 2, 2018, we met with our Advisers and the Members Consultative Group in Philadelphia. We have subsequently revised the Principles discussed at that meeting in light of the comments received.

At the January 2019 Council meeting, we received Council approval of the changes that we made to previously approved Sections as well as Council approval for the remaining Principles. We would then seek member approval of the project at the Annual Meeting 2019.

We are using the following organization of the principles:

Summary of the Principles of Law, Data Privacy §§ 1-2, Purpose, Scope, and Definitions

Section 1 sets out the scope of the Principles. As we note, "[T]he Principles seek to unify U.S. privacy law but not to replace all U.S. privacy law." The Project seeks to move U.S. privacy law toward greater common ground and to close gaps in it. Section 1 is also designed to work well with the First Amendment by its exclusion of certain kinds of personal-data activities.

Section 2 sets out the Project's key definitions. These include the concepts of "data subject," "data controllers," and "data processors." These are important ideas found in U.S. privacy law, although the terminology in the United States is not yet consistent. U.S. privacy law safeguards the interests of "individuals" and "consumers." The law also speaks of "affected parties." It regulates "service providers" and "business associates" and distinguished these entities from the initial collector and the initial collector and user of data. We have adopted the terminology here of the European Union's General Data Protection Regulation because this language is becoming the global yardstick for these concepts.

Summary of the Principles of Law, Data Privacy §§ 3-12, Data Privacy Principles

Section 3 requires a "Transparency Statement." The idea here is to separate out the kind of notice that is useful for individuals, which will be found in § 4, Individual Notice, and the kind of information which is aimed at regulators and the broad public, which is found in this Principle. The § 3 Statement is aimed to assist regulators and the broad public in assessing whether organizations follow the law and to inform them about an entity's policies and practices. The transparency statement also helps bind a data controller or data processor to a regular set of practices in order to prevent it from acting in a purely ad hoc fashion.

Section 4 concerns individual notice. It requires that data controllers provide a notice of rights set forth in the Principles to the data subject. As set out above, these notices are different than the more general "transparency" statement required in § 3. Under some circumstances, Principle §4 requires "heightened notice." There are also some exceptions articulated to this Principle, which permit a data controller to refrain from complying with this Principles.

Section 5 sets out the Consent Principle. It places the obligation for obtaining consent on the data controller and requires that the form by which consent is obtained be reasonable under the circumstances. This Principle also sets out exceptions under which consent must not be obtained from the data subject. These include when there is legal authorization for the data use.

Section 6 establishes a duty of confidentiality. The development of confidentiality has been less than robust, although found in some case law and current discussions regarding relationships of trust in data handling. In our view, it is a very important principle of data privacy.

In § 7, we set out a "use limitation" principle. These tie the use of data to the "Notice" principle (Principle 4). As compared to previous drafts, the change in this version concerns improvements in the drafting of the exemptions to the requirement for consent. The exemptions are now clearer.

In § 8, we express one of the most universally accepted Fair Information Principles, which concerns rights of access and correction. Section 8 expresses these ideas, including an interest of the individual in being able to challenge the accuracy of data relating to her or him.

Section 9 presents principles regarding data portability. When appropriate, an individual is to be able to request a copy of his or her personal data in a usable format. Under the Obama Administration, the White House already had begun to promote data portability in both the public and the private sectors. This idea is also found in the California Consumer Privacy Act of 2018.

In § 10, we develop a principle of data retention and disposal. In particular, when data is no longer necessary for the purposes for which it is collected, it is to be destroyed. Data destruction is to be pursuant to reasonable procedures to ensure that personal information cannot be accessed or made readable.

Section 11 concerns Data Security. It provides for the protection of personal data with reasonable security safeguards against foreseeable risks. It also contains requirements for personal data breach notification.

Section 12 places limits on Onward Transfer. This idea is that a data controller or data processor should only make onward transfers for personal data activities for which the data subject has been provided notice. When a data controller makes use of a data processor, there is a need for a contractual agreement between the two parties to ensure the protection of personal data consistent with these Principles.

Summary of the Principles of Law, Data Privacy §§ 13-14, Accountability and Enforcement

Section 13 develops the idea of Accountability. This concept has been present in information privacy law since the development of the OECD Guidelines (1980). It requires oversight and if governance mechanisms within an organization.

Section 14 develops Enforcement Principles. It sets a series of "factors to be considered in deciding on the nature of remedies, if any, for the violation of a principle." The organizing concept here is to provide a menu of concepts for legislatures and courts to consider in deciding on remedies, or in deciding against their availability. Key concepts include the principle that, to the extent that the law recognizes any remedies for these Principles, they be "effective, proportionate, and dissuasive."

***

As Reporters, we are very grateful for the extensive comments, criticisms, and overall feedback from the Advisers, Members Consultative Group, Council, and members. Every aspect of this Project has immeasurably benefited from these valuable contributions.