30 Years After: The Impact of the OECD Privacy Guidelines
Remarks of Hugh G. Stevenson
Deputy Director, Office of International Affairs
U.S. Federal Trade Commission[1]

Paris, March 10, 2010

Thank you. I appreciate the opportunity to describe the United States experience with the OECD's 1980 Privacy Guidelines. I describe this experience in particular from the perspective of the U.S. Federal Trade Commission (FTC), an independent federal agency and one of several U.S. government entities charged with the enforcement of U.S. privacy laws.[2]

To consider the impact of the 1980 Guidelines, it is helpful to consider the historical context; part of the Guidelines experience was obviously shaped by what led up to them. Hanspeter Gassmann has provided a useful overview and has capably set the stage. I would like in addition to focus on two important U.S. developments that laid the groundwork for the 1980 Guidelines.

The first was passage of the Fair Credit Reporting Act of 1970, a law that addressed notice, use, access, and accuracy as to databases of credit records.[3] The second was a 1973 milestone report issued by a U.S. government advisory committee to the Department of Health, Education and Welfare entitled "Records, Computers, and the Rights of Citizens."[4] This report set out a number of principles that remain relevant today - - "fundamental principles of fair information practice" - - to protect the privacy of information about individuals. These principles appear in the U.S. Privacy Act of 1974,[5] with significant parallels to the principles contained in the OECD Guidelines. Thus, by 1980 many of the principles in the OECD Guidelines were increasingly becoming part of the privacy culture in the United States.

---

[1] Today's comments express my own views and not necessarily those of the Federal Trade Commission or any individual Commissioner.

[2] The FTC has the authority to challenge privacy-related practices within a considerable portion of the commercial sector pursuant to several statutes.

[3] Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., *available at* http://www.ftc.gov/os/statutes/031224fcra.pdf

[4] Records, Computers and the Rights of Citizens, Report of the U.S. Secretary of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems, July, 1973, ("1973 HEW Report") *available at* http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[5] The Privacy Act of 1974, as amended, codified at 5 U.S.C. § 552a, is available at http://www.justice.gov/opcl/privstat.htm.

The principles set out in the OECD Guidelines continue to have an impact in many ways. As to government, many of the principles are directly reflected in such legislation as the Privacy Act, and in numerous other statues, such as the Freedom of Information Act[6], the Electronic Communications Privacy Act,[7] and the Right to Financial Privacy Act.[8]

As to the private sector, the principles appear in numerous sectoral laws, including those relating to financial information and health information.[9] Enforcement of the Federal Trade Commission Act's prohibition against unfair and deceptive practices also often implicates some of the concepts in the Guidelines, for example to preserve the integrity of choices made based on notices provided, and to vindicate the principle of data security.[10]

Looking beyond legislative text, you can also see reflections of the Guidelines' principles. The emphasis on enforcement in the United States has a significant connection to the Guidelines' principles, which highlight the importance of remedies,[11] sanctions, and accountability.[12] This is the case not only at the FTC, but in other agencies, like the Department of Health and Human Services, which is charged with enforcing laws on personal health information, an increasingly important issue given the increasing importance of electronic health records.[13]

---

[6] The Freedom of Information Act (FOIA), 5 U.S.C. § 552, was enacted in 1966, and as amended, is available at http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm

[7] The Electronic Communications Privacy Act, 18 U.S.C. § 2510, was enacted in 1986.

[8] The Right to Financial Privacy Act, 12 U.S.C. 3401 et seq., was enacted in 1978.

[9] *E.g.*, Gramm-Leach Bliley Act (GLBA) (Pub. L.106-102, 113 Stat.1338, codified in relevant part at 15 U.S.C. §§ 6801-6809 and §§ 6821-6827, as amended), and the Health Insurance Portability and Accountability Act (HIPAA) (Pub. L. 104-191 §§ 262 & 264).

[10] A description of the FTC's privacy initiatives, including its enforcement actions, is available on the FTC website at http://www.ftc.gov/privacy/.

[11] Part Four (National Implementation) of the 1980 Guidelines, provides that member countries "should in particular endeavour to . . . provide for adequate sanctions and remedies in case of failures to comply with measures which implement [the guideline's basic principles]." Guidelines, paragraph 19.

[12] The Accountability Principle provides that "[a] data controller should be accountable for complying with measures which give effect to the [other basic principles of national application.]" Guidelines, paragraph 14.

[13] The Department of Health and Human Services (HHS) enforces HIPAA, which applies to "covered entities" that are providers of care, payers of claims, or clearinghouses that support those functions who engage in electronic claims transactions. HIPAA is implemented by several rules, including a Privacy Rule that permits disclosure of individually identifiable information for treatment, payment, and health care operations, but otherwise prohibits disclosures except as authorized by the Rule. The FTC has the authority to challenge privacy practices on the part of non-"covered entities" that violate statutes enforced by the FTC. In addition, both the FTC and HHS recently issued rules relating to breach notification with regard to health information, as provided for in the American Recovery and Reinvestment Act of 2009.

The effect of the Guidelines also appears in self-regulatory initiatives, something that is also encouraged by the Guidelines.[14] The effect of the Guidelines is also evident in the common practice of providing privacy notices.[15] If you look at company privacy policies and industry codes of practice in a number of different privacy-related areas, like behavioral targeting, these have the OECD Guidelines "written all over them."

Thus in legislation, in agency enforcement, and in business practice, a reflection of the Guidelines is apparent. At the same time, we are of course mindful that the world has changed in three decades, and that we face several new realities. Let me highlight three.

First, technological change, and the proliferation of privacy notices, has made the provision of notice and choice more difficult today than it was three decades ago. In the United States we are continuously evaluating the application of current privacy protections to a host of new technology applications, on such broad-ranging subjects as Radio Frequency Identification (RFID), social networking sites, cloud computing, mobile marketing, and online behavioral advertising. Indeed, the Federal Trade Commission is in the midst of an important "rethink" project, a series of roundtables re-evaluating the effectiveness of current models to protect consumer privacy in light of technological and business innovation and trying to determine how best to protect both consumer privacy and the consumer benefits of such innovation.[16] We've seen many OECD participants at meetings of this roundtable project, the third of which will take place on March 17. The U.S. Department of Commerce has also launched a privacy and innovation initiative, which my Department of Commerce colleague, Danny Weitzner, will say more about during the next panel.

The second new reality I'd like to highlight is the exponentially greater amount, and qualitatively different nature, of cross-border data transfers. Different regulatory frameworks governing such transfers increasingly challenge the other core principle in the Guidelines, protecting the free flow of such data across borders. (Remember that these are guidelines "on the protection of privacy and transborder flows of personal data [emphasis added].") We should consider whether the legislative environment currently in place lives up to the Guidelines' vision of free information flow.

Finally, I would highlight the topic of accountability, another principle within the Guidelines.[17] The challenge of "accountability" has evolved—and continues to evolve—as the

[14] Part Four, (National Implementation) of the 1980 Guidelines, provides that member countries "should in particular endeavour to . . . encourage and support self-regulation, whether in the form of codes of conduct or otherwise." Guidelines, paragraph 19.

[15] The Privacy Rule, issued by the FTC pursuant to GLBA, sets forth requirements of the notices that must be issued to consumers in accordance with the Rule.

[16] *See* *http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml*.

[17] Guidelines, paragraph 14.

entities accountable for controlling data have gone from the few in data centers to almost all businesses all the time. This changes the dynamic for both the regulators and the regulated; to take one simple example, think about changes to the challenges of keeping data secure. It also heightens the importance of international cooperation—another key part of the Guidelines.[18]

All these new realities mean we have our work cut out for us. Thank you.

[18] See Guidelines, Part Five ("International Co-Operation").