TECH POLICY NOTES

JULY 2001

United States Begins Accommodation of European Internet Privacy Rules

U.S. companies are observing new rules for privacy protection, but these apply only to European consumers. Beginning this month, U.S. companies must meet the privacy standards of the European Union (EU) in order to do business in Europe. They can do so by certifying that they meet the personal data protection requirements of the "Safe Harbor" agreement between the United States and the EU. The agreement averted a situation where U.S. companies would have faced serious obstacles to participating in European e-commerce. The start of Safe Harbor has serious implications for the privacy debate in the United States.

The EU agreed to Safe Harbor, despite reservations from some member states, as a way to allow the United States to comply with more stringent European privacy standards. The EU's broad regulatory approach to privacy contrasts with the U.S. reliance on sectoral and self-regulation. EU requirements, such as making companies notify consumers that they are collecting data or obtaining consent before data can be collected, are attractive to U.S. privacy advocates. However, critics point out that the EU approach to privacy predates the explosive growth of the Internet and may impede e-commerce in Europe. In part, this reflects a larger difference between the United States and EU over how much regulation is best for economy and society. Less regulation is sometimes cited as a reason for the superior performance of the U.S. economy.

Concern over privacy of personal data, along with the related issue of security, is a crucial obstacle for obtaining the full economic value of the Internet. Recent polls cite concern over privacy as a key reason why the majority of Americans want to "go slow" in developing e-government. These are clearly key issues for law and policy in the United States, but the Congress and the Administration will need to need to pay careful attention to avoid any "unintended consequences" of privacy laws or regulations. For example, a law passed to protect children on the Internet led to the closing of a number of children's sites (a talking railway engine's site, for example) because of requirement for parental consent. Privacy laws, if they are broad, will need to be carefully shaped if they are to avoid creating as many problems as they fix.

Privacy is linked to the Internet security issue since at least some of the data collection is done without the knowledge (or consent) of the target. Protective measures that would alert you to and block a probe of your computer could also block some of the data collection techniques. Effective security enhances control over what your computer runs and whom it communicates with, which would frustrate some of the existing techniques for data collection. That said, effective network security measures would only reduce, not resolve, the privacy problem.

The United States (at the state or federal level) already has an array of privacy laws and regulations governing various industry sectors. The FTC's recent regulation implementing the Graham-Leach-Bliley Act governing financial institutions and privacy is a good example of the sectoral approach. Eventually, the United States may assemble enough laws to form effective protection for privacy, but that has not happened yet. Broad legislation imposing rules similar to Safe Harbor would address of the privacy problems faced by the United States but would face opposition from business groups.

The economics of privacy suggest that there may be a trade-off between long-term gain to an Internet-based economy and immediate cost to current business. In many ways, personal data on the Internet is a "free good," obtainable without payment to the owner. Adapting Safe Harbor could pose problems for some Internet business models. While "B2B" (business-to-business) models for e-commerce are succeeding, many of the dot.coms offering consumer goods and services over the net have run into hard times (one estimate places revenues from sales to consumers as one-tenth B2B revenues over the next five years). Some companies hoped that collecting personal data would allow ads and sales to be targeted to individual consumers and unlock spending on the Internet. It may be too late to help the dot.coms, but collecting personal data from the Internet is still attractive as it can be done cheaply and can provide a wealth of information on consumer preferences. Data collection remains one sure way to generate revenues from Internet activity,

and this may make some in the United States reluctant to move to EU-style regulations. Regulating the use of such "free goods," whether they are grazing lands or air pollution, has always been contentious, and private data is not likely to be different.

It is too early to tell if being forced by the EU to adopt privacy standards will lead companies to adopt similar practices for U.S. consumers. One argument is that companies may find it more economical to use a single standard (i.e., the required EU standard) than to have one standard for Europe and one for the United States. This single standard argument may overestimate the costs of maintaining separate policies.

Concern by consumers over privacy of personal data (along with the related issue of data security) remains a major obstacle to taking full advantage of the Internet. Privacy is likely to be an issue for the next Congress, which will have to weigh the benefits of a broad regulatory approach like the EU directive against the sector-specific, self-regulatory approach used in the United States. Although previous efforts by Congress to legislate Internet activity have not always worked well, a lack of progress in improving privacy protection in the United States may lead privacy advocates and Congress to call for extending "Safe Harbor" to Americans.

Useful Links

http://europa.eu.int/comm/internal_market/en/smn/smn23/s23mn27.htm

http://www.ftc.gov/privacy/index.html

http://www.export.gov/safeharbor/