

Statement of the
Center for Democracy and Technology

Ari Schwartz

before the

Federal Trade Commission
Workshop on “The Information Marketplace:
Merging and Exchanging Consumer Data”

March 13, 2001

Session 5: Emerging Technologies and Industry Initiatives:
What does the future hold?

Utilizing Privacy Controls in Data Transfer Technologies

Summary

Privacy enhancing technologies can aid companies in complying with standards to protect individuals while utilizing the latest data transfer technologies. In particular, there has already been discussion of using existing standards to help individuals and companies repudiate the privacy rules under which they provided the data. It is also likely that the same technologies that are used for data transfer would make it easier for individuals to access information held about them. However — since data transfer happens “behind the scenes” — it is unlikely that market incentives alone will force companies to utilize these technologies. Therefore, in order to protect privacy, it will be necessary to promote baseline standards that will ensure that consumers will receive the benefits of these tools.

Introduction

New standards and technologies are being developed by industry to help companies share information. Meanwhile, technologies are also being developed to help consumers gain more control over their own personal information. One important piece of development is often overlooked: the ability of technologies to help companies play a more responsible role in protecting consumer information. Here are two examples of standards developments that can help companies play a more responsible role:

The P3P Vocabulary

The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. The main original concept behind P3P was to enable browsers to "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P would then enhance user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.

In order to make this standard function, the P3P Working Group needed to find a vocabulary that could express all of the fair information practices — as they are understood internationally — in a very detailed way. Unfortunately, no such vocabulary existed at the time. Therefore, in order to reach a vocabulary that could truly be representative of all of the necessary aspects of all privacy policy, the working group met with companies, data commissioners, privacy advocates, industry groups and others world wide. The result is the multiple-choice questions originally envisioned in P3P use. These questions are:

- Who is collecting data?
- What data is collected?
- For what purpose will data be used?
- Is there an ability to opt-in or opt-out of some data uses?
- Who are the data recipients (anyone beyond the data collector)?
- To what information does the data collector provide access?
- What is the data retention policy?
- How will disputes about the policy be resolved?
- Where is the human-readable privacy policy?

While the answers to these questions were originally designed for business to consumer transactions on the Web, other groups and companies could use this work to help describe other types of data transfers. For example, a company could convert their human readable privacy policy into P3P and then tag all

information that comes in with that policy. Then if the policy changes, data collected after that point could be tagged with the new policy. This would help companies audit their privacy practices and perhaps stop “data spills” or the misuse of personal information from happening. In fact some tools, such as IDcide’s Privacy Wall, are already under development to do this.

Access Standards

Other standards that utilize the eXtensible Markup Language (XML) are under development to help companies share data with other companies. These technologies would standardize data fields and a means to exchange information. Interestingly, these very same tools can be utilized to help consumers gain access to their own information in the hands of others. Simply put, by making data sharing easier between companies, a company is also ensuring that data transfer becomes easier between all parties — including the data subjects themselves.

In the Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security of May 15, 2000 the opponents of online access specifically cited the costs, “including, among others, any required modifications or new design requirements placed on existing systems.” If these new technologies were in place, this would no longer be as large a barrier. The most significant obstacle would be to authenticate and verify that individuals are who they say they are. Since companies would already need a means of authenticating other companies to share information, the only remaining concern would be scalability.

Conclusions

Undoubtedly, companies that utilize these technologies to help give individuals more control over their information and help the company evaluate their own practices. Yet, their existence alone does not necessitate their use. In fact there is little baseline incentive for a company to use these technologies without some set of baseline standards to follow. This is particularly true because these are both back-end uses of standards. Using these tools could make it more likely that a practice that is currently unseen by consumers becomes a privacy concern. Therefore, without further moves to push more companies to be responsible actors, their adoption is somewhat uncertain.