The Dimensions of Consumer Privacy

Privacy is an overloaded word. Privacy to some means Constitutional privacy rights and the United Nations' identification of privacy as a fundamental human right. Privacy to others means the right to be left alone. Privacy to a third group means choice over personal data and the trade-offs in its protection or exposure. An understanding of these dimensions of privacy and the stakeholders in the privacy debates will illuminate the market for privacy in all its complexity.

Those who view privacy as a basic human right will not rely on the merchant to provide such privacy. Consumers who see privacy as something absolute are likely to use customer-specific software to prevent the use of secondary information. However, shopping requires the provision of information: items selected, time of purchase, mechanism of payment, delivery address. Consumers who consider privacy a fundamental right may browse the web but are reluctant to shop on the Internet until privacy-enhanced mechanisms of payment are available..

The second group, those who would be left alone, is not entirely separate from the first. One can want to be left alone and want no exposure of certain personal information. For example, a consumer may be very willing to purchase books but not health-related goods on the Internet.

For those wishing to be left alone the ideal business relationship is represented by a single transaction, which is neither tracked nor used as the basis for any further contact from the merchant. Such buyers are most likely to reject merchants seeking a continuing relationship, merchants that require the creation and management of an account. These consumers would prefer to have each transaction separate and isolated. Intrusive merchant practices, such as opt-out email lists with difficult policies for subscription removal, are the bane of this consumer set.

Still other buyers - the largest group, no doubt - are those who feel that their data are valuable. For these consumers all transactions should reflect a balance between risk and reward. A large number of such people will give data happily for a discount, but would rather not be involved with a merchant that collects data with no return advantage to them.

It is this group that enables businesses such as Amazon to collect personal information with no consumer backlash. Amazon has a particularly lax privacy policy, basically stating that it owns all information and can dispose of it at will. However, the information Amazon stores also serves the consumer. The storage of credit card numbers and purchasing habits are not seen as objectionable because they make shopping easier.

While consumers do not see all uses of the data, consumers do see how the data compiled is of use for both merchant and consumer. Note that several electronic civil liberties groups (including the Electronic Frontier Foundation and Computers Professionals for Social Responsibility) have called for boycotts of Amazon, but these have had limited effect. It is the combination of reliability and customer service enabled by customer data that keeps Amazon relatively safe from consumer backlash.

Thus there are three types of privacy-centered customers: Those who would avoid merchants not providing privacy; those who would avoid merchants that require an intrusive relationship for a simple transaction; and those who simply want to see service commensurate with their data exposure.

Privacy and Security

Distinguishing between the privacy and security markets is critical in understanding the roles of emerging businesses that target the privacy market. The privacy market en masse tends to

overwhelm the security market, because privacy encompasses security. Security means that those who own data control access to that data. Privacy means that the subjects of data either control access or have auditing rights.

The confusion between privacy and security, particularly in financial transactions where privacy has been associated with anonymity and thus fraud, further obscures the view of the privacy market. The complex interaction between security and privacy is further compounded by the use of metaphors (e.g. "Digital signatures") that have confusing or incorrect implications. Increasing privacy usually increases security, but in some cases decreasing privacy increases security.

An example in which increased privacy would create increased security is in the case of Social Security Numbers. Social Security Numbers are widely used for identification numbers, so much so that they have become universal identifiers. Many computer systems use Social Security Numbers because they are unique, and every user has one. For example, Carnegie Mellon University used social security numbers as passwords for each person's first connection to its distributed computing system. The University President Mehrabian never logged in. However, one day an extremely irate professor marched into Mehrabian's office demanding an apology for the president's abusive email. Thus Mehrabian discovered that several undergraduates used his Social Security Number to impersonate him and had been widely using his account to inflame faculty.

While this anecdote may be amusing, it also nicely illustrates that a single identifier should not be widely used. More seriously, by obtaining a Social Security Number a thief can commit identity fraud whereby the thief obtains credit in the name of the victim. Making Social Security Numbers more private would make them more secure.

Of course the same is true of credit card numbers. Credit card fraud is easier to resolve than identity fraud for the victim. However, such fraud is also more common.

Problems with identity fraud can be exacerbated by merchant choices on privacy. For example, Yahoo! requests that users provide a date of birth in order to confirm their identities. The result is that Yahoo! has a large compilation of user names, email, and date of birth. Using email it is possible to obtain real names and thus physical addresses through directory services. Should the same customers use Yahoo! for auctions and email, Yahoo! has a database which is ripe for identity theft even without the inclusion of Social Security Numbers.

Privacy and security conflict in cases of surveillance. Law enforcement, employers, and insurers often want surveillance capabilities for security purposes. Business surveillance of customers is justified on the basis of deep marketing.

However, increased privacy can enhance marketing. Privacy requires that the subject of information know of the compilation of information, and be able to read the information to determine if it is correct. Fulfilling these elements of privacy enhances marketing, in that consumers do not want to know of offers in which they are uninterested.

The classic example is the search for insurance. After an initial search the consumer makes an insurance decision, and thereafter he or she no longer needs additional information or contacts. Merchants do not want to spend marketing resources on consumers who are not interested in a purchase. If customers could edit their profiles in merchants' marketing databases, merchants and consumers would receive greater value. Customers' ability to manage their own data increases customer privacy and company efficiency.

Privacy and security can conflict in the case of auditing. Avoiding this conflict requires designing privacy into the system, rather than adopting a system and attempting to add privacy as

a feature later on. Thus the ability to audit and complete conflict resolution varies between privacy-enhanced systems.

In sum, except in rare cases, privacy improves security. In those cases where privacy does not increase security, privacy increases efficacy or reliability. Calculations about the value of privacy would best include these variables.

Without technical safeguards an institution may be unaware of the data compilations obtained at the consumer level. For example, a General Accounting Office study found that the majority of Federal Government web sites violated Federal electronic privacy policies. In many of these cases the managers simply did not know what data were being collected. Survey forms and cookies were placed on the web by past programmers or long-gone employees. Data were collected and stored, putting the Federal departments at risk for citizen suits yet, there were no strategic reasons for those data collections.

Similarly Federal Trade Commission studies have found that of those sites which post a privacy policy, a significant minority do not follow the posted policies. Thus to trust a site's privacy policy a consumer has to trust far more than good intentions of the owners. The consumer must also trust that the database manager and the web designers are required to meet the letter of the privacy policy on a daily basis.

Customer Privacy and Value

Customers seek both to be served by merchants and to be left alone by merchants. It is this balance that must be addressed when developing privacy software for the consumer market.

Freedom, the early software by Zero Knowledge Systems, did not allow web browsers to shop. Rather, the web browsing software provided anonymous browsing. A similar service was provided by the Anonymizer in the early days of web browsing, and is now also provided by Anonimizer.com

Other companies offer individuals the ability to mange personalities or personas on line. Such self-management software requires a concentration of trust. In the e-commerce arena attempts to concentrate trust in a single entity have failed. For example, First Virtual concentrated all trust in First Virtual, while Ebay offered similar down-market services in which the customer managed his or her own trust. Ebay allows payment mechanisms to be provided by third parities so that users can create distinctive personalities of various levels of trustworthiness.

Mechanisms that prevent the consumers from shopping, or require that all trust be concentrated in a single entity, do not address the core problem of the consumer: how to distribute information in such a manner that is optimal for the consumer.

Conclusions

Consumers who value privacy as an inherent right can choose among the privacy-protecting technologies which will protect that inalienable right. For the larger set of consumers, there is a desire to set the degree of privacy in interactions with a site. A consumer may be more than willing to accept cookies for the purpose of customization but will not want long-term storage of shipping addresses and credit card numbers. By providing consumers with an opt-in option for all marketing emails and minimizing the amount of information collected to that which is necessary the merchant ensures that customers' privacy is maintained. Merchants avoid unwanted marketing messages and business data storage that creates financial and legal risk for no gain. By allowing customers to opt in the merchant selects only those customers who are

interested in the marketing information provided.

As the information economy expands the most valuable software will be that which decreases or filters information.