WHAT PRICE PRIVACY?

A. Cemal Ekin

Not too long ago, Intel introduced their then new processor, Pentium III that caused an unexpected uproar. Many voiced their concern over the built in identification capabilities of the processor. It could uniquely authenticate the computer and through presumption, the user. This unwanted identification was certainly not a welcome addition to the feature-set of the new chip since many users wanted to remain anonymous when they browsed the Internet.

Now, part of this concern is quite legitimate but the rest needs some deeper digging. Clearly, it is every user's prerogative to identify themselves or avoid it altogether. That said, the same users who vehemently opposed this automatic identification idea probably do not even know that their computers may contain other unique numbers that can be traced to their owners. For instance, Ethernet network interface cards, by their very design, contain and must broadcast their ID numbers to facilitate network communications. Furthermore, every user on the Internet, again by design, must have a unique IP number, which can also be traced back. These systems will simply not work without their unique identification schemes. The reason most of us are willing to put up with them probably lies in either not knowing that these numbers can be traced or our willingness to tolerate them so that we can be involved in network communications or use the Internet.

What is the real issue? This is not an easy question and many people have been working both in the industry and in the government to find usable solutions that will satisfy most users. Let us pose a more general question to start the discussion: "In today's economy, is it possible to be truly anonymous?" We can imagine using cash for all transactions so that our checks or credit cards will not identify us. This surely makes our lives much more difficult without really giving us the

desired level of anonymity. Most employers pay either with checks or through direct deposit both of which require at least one bank transaction. Of course, there is always the Social Security number that we need to obtain before applying for a job. Let us not forget the surveillance cameras that banks use to record their transactions and those many retail establishments use to track shoppers' movements. Most of this kind of information is collected without our consent and certainly jeopardizes our desire to remain anonymous. Remember that even a reclusive character like Ted Kazinsky, the alleged Unabomber, could not maintain full anonymity.

Then, what is the problem? Is it our stubbornness to resist providing personal information when asked or our concern for its proper use after its collection? So far, neither the banks nor the retail establishments that use surveillance cameras have developed a way of analyzing the video information. This kind of information does not have any economic value that may result in its resale. So, when this kind of information is collected, we usually do not mind because it does not identify individuals with traceable contact information. This is certainly comforting, at least until someone develops an accessible method of analyzing video data.

Most of the time, we also do not mind plunking down a credit card for a purchase we make. After all, convenience has a price and credit card companies give many incentives to use their cards. Nor do we hesitate too much when asked for our names when purchasing a plane ticket. Again, we make an implicit trade-off between the utility of flying versus other modes of transportation and in addition, let us not forget the security related issues here. So, we have been "trading" our personal information in the real world for many years as long as we consider this trade fair. Why, then, has the Internet heightened our awareness of privacy, anonymity and protection of personal information?

There are probably many highly interrelated reasons for this phenomenon. The first may be the perception of the Internet, at least in its early years, as a haven for hackers lurking in the electronic mud waiting to do unsavory things. Early on when this technology was still

in its infancy nobody knew much (or anything) about secure servers let alone use them. This created truly an insecure environment for any kind of information and certainly for sensitive personal data. Although these problems have since been resolved and Internet transactions can be very secure, the initial perception persists.

Second, Web users have realized that personal information has value and Web sites should at least promise "appropriate use" of this information before the users provide it. Collecting this kind of information on the Web, to a large extent, is easy and inexpensive. On the other hand, with the use of new analytical techniques like data mining, owners of consumer information could gain behavioral insights and use the same information for unsolicited promotion. This is not intrinsically bad. In fact, there may be a host of benefits to both the consumers and the sellers.

Third, in the real world dealing with similar problems over the years has resulted in a protective legal and regulatory system with necessary authority given to appropriate organizations. In contrast, there are no counterparts to this structure in cyberspace. Combined with the easy and affordable nature of setting up a Web site to both collect and disseminate information, this makes it easy to lure unsuspecting individuals into financial or psychological losses. I personally know one individual who lost $2,500 after a transaction on the Internet. This individual's reckless behavior notwithstanding, losing this kind of money through a similar transaction in the real world would have been nearly impossible.

Our challenge lies in establishing the infrastructure of transactions in cyberspace so that it serves all without severely inhibiting commerce and marketing but protects the rights of the individuals. People from watchdog organizations, trade associations, technology companies and of course, the government have been working to find the answers to these highly complex problems.

Let us hope that a solution emerges sooner rather than later.

See the following sites for additional information:

Electronic Frontier Foundation: http://www.eff.org/

Trust-e: http://www.truste.com/

The Better Business Bureau: http://www.bbb.org/

The United States Senate: http://www.senate.gov/

U.S. House of Representatives: http://www.house.gov

This Editor's Choice column originally appeared on September 3, 1999 on CourseLinks Marketing on the Internet section the content of which was maintained by the author.