



A Brief Introduction to iPrivacy

Jonathan M. Smith

Chief R&D Consultant, iPrivacy.com

322 8th Avenue, New York, NY 10001

(presentation for Paris Conference, September 25th, 2001)

1.0 Privacy Threats on the Internet

The Internet software was originally designed as a research artifact for investigating interoperability amongst computer networks. The approach chosen was packet-switching, as that approach seemed general and offered many advantages in terms of multiplexing, robustness and flexibility for applications. An important characteristic of the technology is that the network source and destination addresses for a packet are contained within the packet, so that localized decisions (such as routing decisions) can be made while the packet is in transit. This local decision-making is a source of considerable robustness.

Support for the effort was provided for over twenty years by the U.S. Department of Defense's Advanced Research Projects Agency (DARPA) and led to a remarkable community, cooperating towards construction of this common system. Since it was a community, many tools and systems were available for diagnosis, location and collaboration. Other than normal authentication for attached computers, very little support for security (other than the robustness engendered by the packet switching technology itself) and privacy was created, as there really was no point to building such facilities – they were, for the most part, just an afterthought for the research community, and in many cases viewed as an impediment to getting the “real work” done.

The Internet became commercialized as a result of two innovations. First, in the early 1990s, networking researchers were investigating possibilities for LANs and WANs with much higher performance (by a factor of 10 or 100) than had been seen outside the laboratory. An example of this was the U.S. “Gigabit Testbed” program, which was a resounding success, demonstrating computers communicating at speeds in the range of 1000 megabits per second. The new technologies were quickly embraced by the commercial world, as well as by the Internet community. The second innovation was the World Wide Web, developed in Europe at CERN, and browser technologies that could exploit the hypertext links provided by the technology. These two innovations are deeply related, as the large bandwidths available on LANs and WANs allowed complex hypertext, including pictures, to be transported and viewed, particularly amongst the highly networked scientific laboratories where the network technologies were first deployed.

Browsers are applications that use the Hyper Text Transport Protocol (HTTP) to send and receive strings of data. A typical request from a browser might be Universal Resource Locator (URL), resulting in the response of an object, such as a page or picture, available at that URL. The URL consists of two parts – a server part and an object part –

so that the server can be located on the Internet, and the object located on the server. To permit stronger collaboration amongst servers and browsers, the notion of a *cookie* was developed as a way of preserving information about how the browser's user had used the service in the past, for example to indicate preferences for display formats.

This combination of technologies, and the emergence of commercial firms selling browser technology (most notably, Netscape) led to a huge explosion in services available on the Internet, and large amounts of investment designed to capture the minds and money of the users of the new medium. A variety of firms were established with the joint goal of initiating a service, and capturing data about customers that were useful for future relationships and products the company might develop. This business model was readily enabled by the browser and Internet technologies, as browsers conveniently stored cookies that could be used to record user behavior, and Internet Protocol (IP) addresses were readily available from the user's packets. Finally, as a result of the exponential decrease in cost of storing data, large databases of information about user behavior (viewing, purchasing, timing, *etc.*) could be recorded, retained and used to model the user in ways which could improve marketing and sales, and thus increase profitability.

Unfortunately, the mechanisms used by these firms, which offered to marketers a previously unseen capability to gain insight into customer needs and personalize services, have an enormous downside [1]. That downside is loss of privacy, and while the actions eroding privacy are still underway, technological approaches have been developed, and are being commercialized, to provide many of the advanced services of the World Wide Web while preserving customer privacy. iPrivacy is commercializing technology to preserve privacy.

2.0 A Short History of iPrivacy

iPrivacy was founded in 1999, in response to the exploitation of Internet features as a means of violating consumer privacy. The company goal was to provide *privacy*, as opposed to *anonymity*, a service desired by some. Privacy, for iPrivacy, is the promise that no additional information beyond what is provided in everyday transactions would be surrendered when using the Web for purchases. In analyzing these transactions, it became clear that the three forms of personally identifying information (PII) common to all transactions were: (1) Web/Internet-related information, such as cookies and IP addresses; (2) financial information, such as credit card numbers, and; (3) address information, used for physical delivery of the merchandise.

After some exciting and intense analyses, we concluded that electronic cash was not likely to be viable in the near-term future, as it required some challenging operational issues to be overcome, such as consumer use and merchant acceptance. Credit cards were, however, widely used and supported by a robust technology infrastructure [2]. Further, the institutions providing the cards (issuers) had already developed a relationship with customers based on service, and managed risk by modeling customer behavior (this is used, for example, to detect fraudulent use of a credit card). The bottom line is that customers already surrendered significant PII in exchange for the bank's short-term loan of capital for purchases. I'll discuss the shipment and Web solutions in the next section, but the analysis of the financial system demanded a credit card solution, and this made banks the natural customers for a service. They had several incentives: (1) the

technological changes necessary to provide this service were small; (2) they already had business models to sell advertising to customers with purchase/demographic statistics; (3) they deeply did not want to be “disintermediated” from Internet transactions, and would like to have more control of the customer data, rather than less; and (4) banks have a long history of providing privacy for their customers. A marketing study was commissioned, done by a leading firm, and the results in summary were that the service was very desirable to the most profitable customers (those that maintained a balance on the card) and that many customers were not using the Internet due to privacy concerns. What this suggested to iPrivacy was a marketing effort based on increasing market share – to capture these potentially profitable transactions from customers not making purchases due to privacy concerns. This was the strategy (of course there was more, but this was the high level strategy) we undertook.

3.0 Proxying for Privacy

Our consumer privacy solution repeatedly used the principle of *proxying*, which meant an intermediary role in Internet, financial and shipping portions of a purchase and its fulfillment.

The Internet proxy solution was logically quite straightforward, while involving a substantial amount of technical work. Editing the HTTP headers allowed removal of cookies, both for sending and retrieval. It also provided a convenient locus of control for other editing functions such as eliminating active content such as Javascript and Java, if desired. This editing could be done on the client machine or a server, but we placed it on a server system for two reasons. First, we already needed a server, since we need to proxy IP addresses (so that interactions appear to be coming from the iPrivacy server rather than the user host). Second, the server provided some advantages in time to deployment and software engineering. The last component addressed in the Internet space was electronic mail. Here, we examined a variety of solutions, ranging from e-mail forwarding to an iPrivacy-provided Web mailing system, in the style of systems such as Hotmail. We used the latter approach in the deployed system, as we believed it minimized risks due to user error, always a concern in such a system.

The shipping solution was to create an iPrivacy-generated address for use in the transaction. One could imagine this as “iPrivacy customer #65783246, Anytown, USA”, and not be far off the mark. The main idea here was to provide an encoded address that could be interpreted to ship the package. We had arranged with the US Post Office to coordinate such a delivery system, allowing for all normal activities by postal inspectors while preventing the Internet merchant from determining the customer’s home address. The merchant would see many packages shipped to iPrivacy but remain unable to determine the final recipient of the package. E-mail confirmations, *etc.*, were handled by the Internet e-mail proxy solution described above.

The financial space solution seemed to us to be simplest of all. The banking system (particularly credit card processing systems, for both cost and performance reasons) are highly automated. There are already many embedded computing steps in a card transaction, such as charge approval, currency exchange and fraud detection. Thus, adding a feature (we designed a set of these, each of which preserve privacy) to the card purchase process appeared to us to represent a relatively simple programming task, since

it could be completely managed by the issuing bank. An example of such a solution would be the creation of a single-use credit card number, the validity of which would be verified by the acquiring bank (the merchant's bank) but would only be true for this purchase. Mapping such a number to an account for billing is straightforward. This was confirmed in technical discussions we had with banks as a part of the marketing process for our service.

4.0 Experience in the Marketplace

Our initial marketing efforts were *extremely* well-received. Banks saw the Internet as a new space in which to make money, and as an interesting new marketplace in which they did not want to fall behind. Autumn and Winter of 1999 and Spring of 2000 were spent performing demonstrations at top issuer banks as well as to potential collaborators. Interest was very high and motion toward a trial of the service was very rapid, as the banks were forcing themselves to behave in a more agile fashion in the new space. Several suggested that we separate security functions from privacy functions in our service (they wanted security first, and then privacy would be value-added) but we felt that our business model was privacy and that was our true offering, so we did not follow this up.

In later Spring 2000, the so-called "Internet Bubble" burst. The effect this had on our business was profound. The natural risk aversion of the banks returned, with overwhelming speed. With the "Bubble's" bursting, their desire to lead effectively evaporated, causing any trials to be put on hold. While discussions remained active, enthusiasm for trials diminished and commitment of resources seemed impossible. Our market share based model apparently seemed less compelling, as there was not a direct impact on the bottom line.

Nonetheless, having working technology, a powerful intellectual property portfolio (we have six patent filings), experienced management and technical teams, and a societal need have proven attractive. We have a co-marketing deal in place with First Data Corporation (FDC), the major transaction processor, and we have a 4Q in-market test with a Top 5 issuer bank. We still intend to do well by doing good, making a business out of protecting against a societal threat – one that we believe to be of the first order.

5.0 Opinions and Conclusions

Law cannot keep pace with technology, although well-made law can anticipate some (although certainly not all) technological progress. In the U.S., at least, the privacy-invading technology has far outstripped the understanding of the policymakers as well as consumers. It is clear that when consumers are educated about privacy risks, they choose to remain private unless some inducement (such as a coupon or discount) is provided as an incentive to provide PII. Consumers severely undervalue provision of their information, in comparison to its value to commercial enterprises. A clear demonstration of this is frequent-flyer mileage offerings, which cost almost nothing to provide. We believe that while consumers desire privacy, they do not wish to pay for it – they expect it. This has made the Internet privacy "business" space challenging – many of our

competitors have either ceased operations (*e.g.*, Privada) or altered their business proposition (*e.g.*, Zero Knowledge Systems) to reflect this.

We, on the other hand, continue to operate in our original space, while expanding our offerings to include government web sites (for citizens who wish to be private in their interactions with the government, such as perusal of Web sites for tax amnesty, *etc.*) and health industry activities, such as those covered under the Healthcare Insurance Portability and Accountability Act (HIPAA). These thrusts recognize that in the U.S., regulation is a stronger (and thus more immediate) motivation than pure economic self-interest.

We welcome inquiries from collaborators and possible customers world-wide; please send electronic mail directly to our Chief Executive Officer, Mr. Ruvan Cohen, at ruvan@iprivacy.com, our Chief Technology Officer, Dr. Salvatore Stolfo, at sal@iprivacy.com, or call us on the telephone at (212) 367-8895, or contact us via regular mail at the address given above.

Thank you for your attention.

References

[1] S. Garfinkel and D. Russell, “*Database Nation: The Death of Privacy in the 21st Century*”, O’Reilly and Associates, 2001.

[2] D. Evans and R. Schmalensee, “*Paying with Plastic: The Digital Revolution in Buying and Borrowing*”, MIT Press, 2000.