Privacy-Enhancing Technologies for Internet Commerce

L. Jean Camp and Carlos Osorio

August 2002

RWP02-033

Privacy-Enhancing Technologies for Internet commerce

L. Jean Camp
jean_camp@harvard.edu

Carlos A. Osorio
carlos_osorio@ksg.harvard.edu

Kennedy School of Government
Harvard University
Cambridge,MA 02138

Key words: trust, security, privacy, e-commerce

Abstract – We examine privacy-enhancing technologies based on the consistency of the business plans, technology, stated objectives, and the concept of privacy as embedded in the technologies. Three distinct trust models result from the three distinct concepts of privacy: a right of autonomy, a right to seclusion and a right to property. We use these trust models to segment the privacy market and classify the privacy-enhancing technologies. The Anonymizer and Zero Knowledge's Freedom were built as technologies to enhance autonomy, while Privada Control, iPrivacy, and Incogno SafeZone are built to provide seclusion. Microsoft's Passport is built with an assumption of privacy as a tradable property right.

Security, privacy, and authentication are intertwined and sometimes confused in the privacy market. We argue that the creation of new trusted third party is not an effective strategy. In the case of creating a trusted third party, autonomy-based products have been more successful than seclusion-based products, despite the wider array of services offered by seclusion services.

Conceptions of Privacy

Privacy is a critical element of trust (Camp, 2000; Boston Consulting Group, 1997). The extension of information is a canonical definition of trust in sociological experiments to determine trust in computer-mediated environment (e.g., Abric & Kahanês, 1972; Weisband & Kiesler, 1996). Privacy is an overloaded word. In order to examine the proposal for privacy-enhancing technologies (PET), we begin with the fundamental understanding of privacy as three distinct rights: a right of autonomy, a right to seclusion and a right to property. (Camp, 2000) An understanding of these dimensions of privacy and the stakeholders in the privacy debates will illuminate the market for privacy in all its complexity.

Privacy to some means Constitutional privacy rights and the United Nations' identification of privacy as a fundamental human right. Those who view privacy as a basic human right will not rely on the merchant to provide such privacy. (For the foundation-building article on privacy as a right see Warren, S. and L. Brandeis, 1890.) Consumers who see privacy as an 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 not likely to shop on the Internet until privacy-enhanced mechanisms of payment are available.

This work was funded in part by NSF CAREER Grant # 9985433 and a grant from the East Asian Institute at Harvard.

Privacy to others means the right to be left alone. (For the definition of privacy as a tort, wee Prosser, 1941.) The second group, those who would avoid unwanted contact, is not entirely separate from the first group. One can want to avoid unwanted contact and want no exposure of certain personal information. For example, a consumer may be very willing to expose personal preferences about the purchase of books on the Internet, but not about health-related goods.

For those wishing to avoid unwanted contact, the ideal business relationship is represented by a single transaction that 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, or 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.

The third group of buyers are those who feel that their data are valuable. (For a solid theoretical argument for privacy as a property right, see Mell, 1996.) 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 third group that enables businesses such as Amazon to collect personal information with no consumer backlash. The privacy policy of Amazon is that the company owns all customer transactional information and can dispose of it at will. Amazon has not focused on reselling data, but rather on using data for lock-in and customization. Thus, the information Amazon stores serves the consumer. The storage of credit card numbers and purchasing habits are not seen as objectionable because they make shopping easier. The personal data are exchanged for service. Therefore, when some called for a boycott of Amazon, although some organizations redirected their bookstores, the call was not widely heeded. The boycott calls came from organizations which view privacy as seclusion or autonomy – the Electronic Freedom Foundation, Computer Professionals for Social responsibility and the Free Software Foundation. Thus, the privacy policy choice of Amazon should be seen not as existing along a single axis of trust or privacy, but rather in the three-dimensional privacy space.

Conceptions of Privacy

Having provided on overview of the three concepts of privacy, we propose a set of business elements that reflect these conceptions. In particular, the business variables are based on the privacy categories and include the generation of retention coupled with the cost of switching, openness in the form of code availability, and the existence or details of pricing methods for consumer sensitive information. We do not claim that these are the determinants of trust, but rather that these are the determinants of privacy which is itself a single element of trust.. We conclude by summarizing the coherence with respect to the business model, the stated privacy model, and the technology. In particular, we classify those models according to their underlying concepts of privacy: autonomy, seclusion, and property.

Privacy-enhancing solutions for e-commerce are technical representations of a perception of the meaning of privacy. They are the result of the interaction between a specific bias toward privacy and the capacity to build specific technology within the framework created by current business practices. This bias is then embedded in the design of the solution's business plan and a technological model. Information technologies and, in particular, privacy-enhancing solutions for

electronic commerce respond to this reality. The correspondence between business plan elements and privacy are shown in the following table.

Concept of Privacy	**Market Implications**			
	Surveillance	Transparency	Switching Costs	Distinct Issues
Autonomy: watched people are not free	Core issue	Right to examine code	Free action requires switching	May not shop on the Internet
Seclusion: right to be left alone	Acceptable, as long as no contact	Only the outcome matters	Ability to end contact	Not seeking relationship
Property: data are valuable	Must be fair exchange	Competition is adequate for oversight	Expected business practice	Will trade data for convenience

Business Plan and Embedded Concept of Privacy

For those who view privacy as autonomy, issues of governance are foremost. Trust is not likely to be extended lightly. In order to maintain autonomy, trust should be minimized. Thus, the ability to examine the code as an individual or to have chosen agents examine the code is critical. Similarly, surveillance is the core of autonomy. Thus, third-party surveillance is critical. Furthermore, given that freedom of action without surveillance is essential, users must be able to switch between privacy providers. From such a perspective, the technological implementation (Stallman, 1984; Lessig, 2000) creates a new reality through a set of implicit and sometimes undocumented, but to inescapable to most users, rules.

For those concerned with privacy as seclusion, the critical element is the ability to refuse contact. Thus, surveillance is not a critical issue, as long as the purpose of the surveillance is not to enable future, potentially intrusive, contact. Because the ability to avid unwanted contact is important, the user concerned with seclusion would theoretically value the ability to end contact with the privacy provider as well as the merchants associated with that provider. Switching costs matter here, but less than in the autonomy case. Transparency is less of an issue. Seclusion is not a fundamental right, thus the ability to examine a product at the detailed code level is less important than that the product simply work.

Where data are the property, surveillance matters only in that there is a fair return. Surveillance for the sake of surveillance is not acceptable; however, surveillance for explicit reasons, such as improved or personalized service, is reasonable. As for transparency, as long as there is not false representation of a contract, then there is no issue. Competition should serve as adequate oversight. Similarly, in the world of commerce, switching costs are to be expected.

Privacy violation creates business risks. On the day that the Federal Trade Commission announced that Geocities had substantially violated the privacy of its customers the value of Geocities stock plummeted. The worth of Geocities stock fell nearly $1,000,000 for each minute that the stock market remained open. The value of Geocities was in large part its customer relationships, its goodwill. An FTC agreement allowed Geocities to maintain business at the low price of a privacy policy. Geocities stated that the settlement would in no way harm their business practices; which clearly illustrated that the privacy violations were unnecessary as well as expensive.

Similarly, Intel learned the value of privacy in the release of its 1999 commerce-enhancing user identifier in the Pentium III chip. Intel released a chip with a unique identifier, which could not be disabled by the user. Approximately three hours after a boycott of Intel was announced by electronic civil liberties groups Intel posted software enabling consumers to remove the identifier.

In both the Geocities and Intel cases, the merchant was requesting something of value from the user that was little or no value to the merchant. Intel had no plans to profit from the identifier; it was simply easy to add. Geocities' success did not depend on the success of marketing the secondary information provided by customers. In both cases the merchant took risks to enable increased data compilations that were of little or no use in the daily business of the merchant

The compilation and, maintenance of data are expensive. The potential for legal action or customer reaction to errors in privacy calculus can be considerable. Furthermore, the Federal Trade Commission continues to investigate companies with respect to the existence of privacy policies and compliance with those policies. Increasing customer privacy can be a way to reduce risk.

Using these variables and the observation that the design of resolution mechanisms are the most common source of conflict between anonymity and atomicity, we identify the following critical variables: reliability (based on atomicity, consistency, isolation, and durability, or ACID), security (Camp, 2000), consumer switching cost, existence of surveillance, and transparency.

Analyzing the Privacy-Enhancing Technologies

In this section, we apply the framework to the analysis of Zero Knowledge's Freedom Internet Privacy Suite 2.0, Privada Control, iPrivacy, The Anonymizer, Microsoft Passport and Incogno SafeZone[1]. We begin each section by describing the characteristics which cause the technologies to be classified as offering privacy as autonomy, seclusion, or property right. We describe the markets sought by the companies offering the PETs and offer our thoughts on the technology provided. As a caveat, all the descriptions here are based on publicly available information, and thus have limited technologic details.

Autonomy-Enhancing Technologies

The autonomy-enhancing technologies offer the user the ability to access information without surveillance. These services provide full time protection from information leakage, and thus disable many of the technologies used for shopping: java script, cookies, and ActiveX. Figure 1 illustrates the flow of data characteristic of an autonomy-protecting technology. Note the user data (represented by the book) remains under the control of the user.

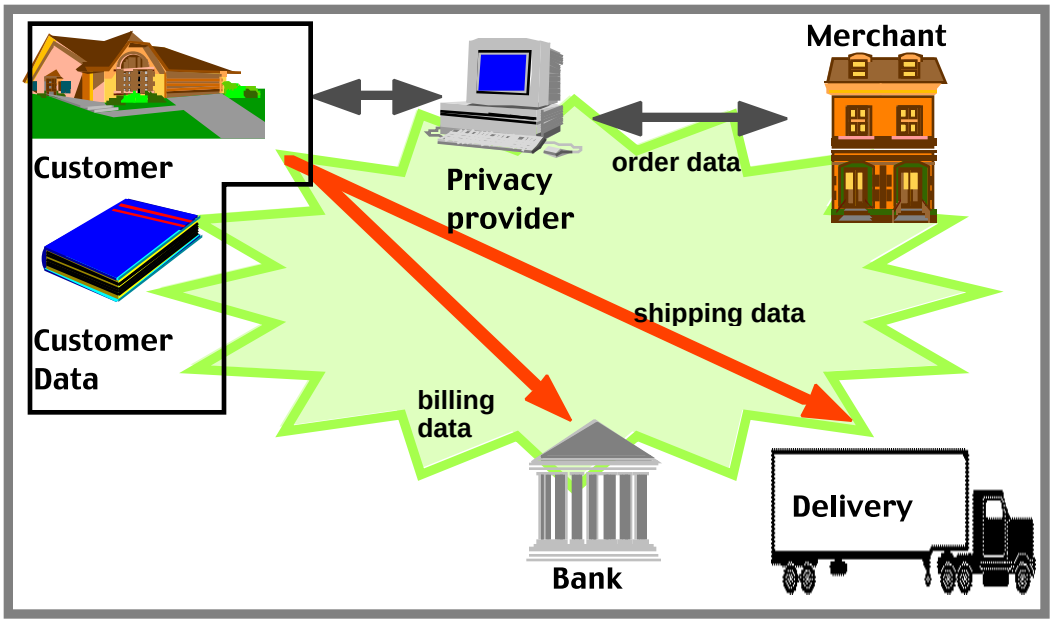

Figure 1: Autonomy Protecting Services Assure Users Control over Their Own Data

Autonomy-enhancing proxy services are distinguished from seclusion–enhancing proxy services by scope (covering all transactions) and scale (during every connection). Autonomy-enhancing technologies do not offer dispute resolution services as such services require the compilation of information for dispute resolution if common commerce mechanisms (e.g., Pay Pal or credit cards) are used.

A rough description of the transaction is as follows:

1. Customer obtains software
2. Customer configures software and establishes an account.
3. Encrypted information tunnels through PET provider
4. PET provider stores no customer data

The Anonymizer

The Anonymizer was initially a student project, implemented by Justin Boyan to provide protection for himself and his associates when browsing beyond the Carnegie Mellon Internet. Thus, the Anonymizer is the oldest of the PETs available for the World Wide Web. The Anonymizer is concerned with solving the privacy problem first and the shopping problem second. The technology is not so much concerned with preventing future contact from merchants or spammers, but with the micro data surveillance to which browsers are subject when accessing servers. It provides no shopping support because shopping support requires the exchange of transactional data. The Anonymizer has no interest in customer data, and is not in the business of dispute resolution. Thus, the issues of atomicity are not relevant.

Any user can access the right to browse without leaving data at sites. However, as a business model the Anonymizer offers enhanced data management including anonymized email accounts.

The Anonymizer provides a system that provides privacy and anonymity by two approaches. First, it provides a proxy server. Second, it provides software-based solutions to manage security at the PC level and provide additional security features to its web-based services, including cookie-management software and auditing tools.

The Anonymizer offer most of its source for download and examination however the availability of source is more an accident of birth than a purposeful strategy. The Anonymizer pricing model, however, treats privacy with respect to commerce as a civil right that can be enhanced by payment, and offers differing levels of service. However, the lowest and most basic level of privacy is provided free for all users. The free services provide for the ability to read and, using basic web forms, write anonymously on-line. The Anonymizer also encrypts transmissions from the user and thus prevents the owner of a users' intranet from observing web-based interactions.

Zero Knowledge

Zero Knowledge is unique in that it is the only company committed to open source in principle. Compare this to the open source provided by the Anonymizer, which offered open source early on as a function of its academic origins. Open source implementation means that any difference between stated goals and actual implementation would be clear. Zero Knowledge understands privacy as a right. Thus, the solution offers the user total control over their own information and empowers the users against even network service providers. The solution functions on a pseudonym system in which the user can buy different pseudonyms, or "nyms," that have limited duration. All users get a proxy bypass service, an anonymizing proxy service, and the ability to monitor and reject third-party cookies at a site-by-site level.

Zero Knowledge is unique in that it allows for full anonymity of the customer to Zero Knowledge as well as to the merchant. Because privacy is a right, the software is available for download and subject to complete user examination. The client can buy up to five pseudonyms a year. The system is relatively easy to use, has low switching costs, and is very interoperable, which is consistent with ZNK's principles. Transactions are promised to have ACID properties; however the first version of Zero Knowledge's software does not allow shopping. Zero Knowledge has the strongest cryptographic technological potential for atomic and anonymous transactions, given the extensive published work by the chief technologist (Brands, 2000) on anonymous and pseudonymous implementations of public key infrastructure.

Zero Knowledge discontinued its anonymous re-mailer service because the cost of supporting an overlay network was too great. Zero Knowledge found rave reviews and many users for its products, but not many would pay for the 'nyms. Now Zero Knowledge is repositioning itself as a risk management company. Based on the observation that privacy policies are rarely implemented by database and web designers, Zero Knowledge offers companies the ability to audit their own data collection and implement administrative policies in technical choices.

Seclusion-Enhancing Technologies

Seclusion-enhancing technologies offer the consumer a trusted third party who promises not to contact the consumer and allows the consumer to choose to discontinue contact with any other merchant. The consumer remains the decision-maker. Seclusion providers differ from autonomy providers in that there exists a trusted third party who stores some data. Figure 2 illustrates the flow of data in a typical seclusion-providing technology. Note the control of the user data (again represented by a book) is now shared with the PET provider. The shared control denotes both

contractual requirements and the ability of a user to choose to end contact and data sharing with any merchant using the PET. The consumer can select merchants to contact, or refuse contact. However, most of the consumer data are available to the seclusion provider, who keeps vital data to provide dispute resolution in the case of failed transactions.

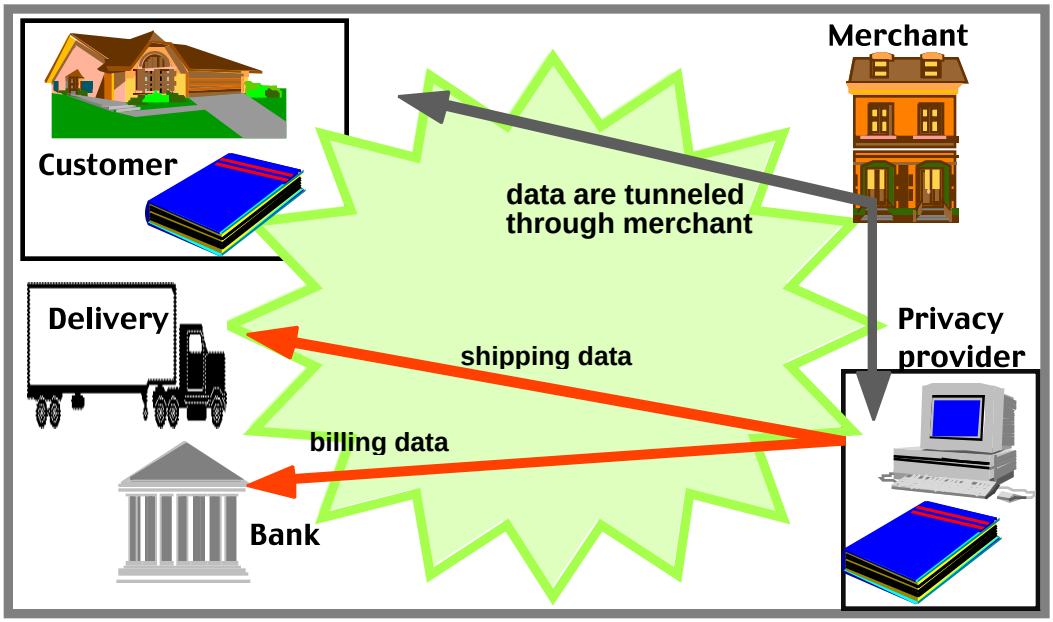

Figure 2: Seclusion Protecting Services Manage Users Data to User Contracts

A rough description of the transaction is as follows:

1. Customer obtains software
2. Customer configures software and establishes an account.
3. Encrypted information tunnels through PET provider
4. PET provider distribute data between provider & customer
5. In case of dispute, customer provides linking data to PET
6. Pet resolves dispute using linked data
7. PET deletes linked data

Thus there is a trust model where increased transactional reliability is balanced with decreased privacy. While anonymous atomic transactions (Camp, 2001) requiring identity exposure for dispute resolution is common in otherwise anonymous payment mechanisms. (Chaum, 1988; Rivest & Shamir, 1996).

Privada Control

Privada, whose name is the Spanish word for “private,” was an early entrant in the PET industry and offered its services primarily to Internet Service Providers (ISPs) and network services providers. ISPs were concerned with market share because broadband technology providers required the use of associated ISPs. Privada offered a way for ISPs to differentiate themselves and build upon the trust relationship presumably established with customers.

Privada offers users a way to interact with merchants without disclosing information except in the case of dispute resolution. Essentially Privada creates a secure virtual private network (Privada Network) with its business clients, who can then provide the client-side software to their respective clients. Privada does not charge users, and places the responsibility for integrating the payment software with the business clients, not the end user. By distributing the cost of running the virtual private network across multiple business services, Privada avoided the high costs incurred by Zero Knowledge.

Privada makes the software easy to install and use by putting the burden in the companies' hands. Their business plan, however, may result in great switching costs for the end users if the user changes ISPs. According to Privada's business plan, if the consumer prefers a higher level of privacy, then the only choice for the customer is to change ISPs. Changing ISPs requires a change in email and a change in URLs for any material published on the Web. Thus, Privada offers ISPs an opportunity to use privacy protection to enhance client retention and justify higher associated switching costs.

Privada's claim that privacy as autonomy is supported by their product is undermined by the business model. The end-user as a consumer may incur high enough costs so as to diminish autonomous behavior. Furthermore, the user's data are visible to the ISP, who is responsible for providing dispute resolution information that requires, of course, the storage of information. The ACID properties of transactions depend on each affiliated company, with the analysis of credit card ACID properties as explained in Camp, 2000. Credit card transactions are atomic, durable, and consistent but not isolated. Durable commitment may require several months of processing in the case of complaints. Credit card transactions are not private.

iPrivacy

iPrivacy offers a proxy for shopping and browsing. As iPrivacy has proprietary technology, some of the cases where apparently conflicting statements are made will be identified with no other comment. Only publicly available information is used in the analysis.

iPrivacy offers the possibility that the Internet should be as private as in the offline world. However, the offline world is not clearly defined. Is this an offline world where every business develops its own database, or the off-line world where automated financial processing does not exist? Is this the offline world of cash or the offline world of credit rating companies?

Since <merchant, email, identity> tuple email goes through iPrivacy, and portals usually know the traffic which passes through them, it is reasonable to assume that iPrivacy has the ability to track each purchase.

iPrivacy functions as an intermediary for the customer and the companies with which the customer interacts. As iPrivacy has proprietary technology it is not certain if iPrivacy has the ability to view all customer data; however, iPrivacy has no advertised business plans to profit from any data compilation. iPrivacy does hold the customer data for the purposes of dispute resolution; however, there must exist information linking customer to purchase in some locale.

With iPrivacy, the customer downloads software which serves as client-side software for shipping and transaction-processing companies. The iPrivacy solution is licensed for credit card and shipping companies, again with the premise that offering customers privacy is as effective as customer data analysis for marketing. For credit card and other transaction processing companies, the advantage to iPrivacy is that it removes the ability of merchants to implement replay attacks.

Here the system generates encrypted data for the merchant and shipping companies, so each one knows a pre-determined minimum of personal information required for performing its activities. With a transaction-oriented approach, the system does not provide anonymity but rather seeks to decrease the merchant advantage in customer tracking information. Thus, the credit card company always has access to all customer information, including goods purchased.

In contrast to Privada, the iPrivacy customer could easily change ISPs or maintain multiple email accounts as long as the billing and credit information provided for a transaction is correct. Of course, the user cannot change PET services, and this lock-in is critical to iPrivacy's success. iPrivacy increases the switching cost to credit card providers because these clients must re-establish the iPrivacy transactional relationship. Transactions have the same ACID properties as with a credit card; atomic, durable after sixty days, consistent, not isolated.

iPrivacy offers dispute resolution services either through storage of hashed information or through conditional and therefore reversible anonymity. Regardless of the dispute resolution practices,, it is certain that iPrivacy views privacy as a seclusion and further confuses privacy with security in its offerings to customers. If iPrivacy does function as a proxy, then iPrivacy has the ability to observe and store customer user habits. According to their business model, iPrivacy could hold customer browsing data to sell analyses to business clients, as opposed to providing customer control over information, as is the case with Zero Knowledge.

Incogno SafeZone

Incogno offers a proprietary solution, similar to those of iPrivacy and Privada. However, where Privada targeted network service providers and iPrivacy has targeted transaction processing companies (e.g., banks and credit card companies), Incogno has targeted privacy-sensitive businesses. Incogno also focuses on the risk to merchants when privacy is a right. For example, Incogno mentions the European Safe Harbor controls on its web site.

The Incogno product SafeZone allows merchants to tailor levels of privacy according to customer or offered service. For example, Amazon may want to offer higher levels of privacy to those selecting books on mental health than those purchasing gardening texts. Thus, Incogno serves as a trusted third-party that manages the relationships between the credit card company, the merchant and the shipping company. Incogno restricts the information the merchant wishes to collect from its customers and the details available to the credit card company. Since credit card companies are a major source of consumer data, this is an important element to Incogno’s offering to consumers. Incogno maintains that Incogno itself can view no customer data.

Incogno is explicit about the method in which it provides pseudonyms to merchants. Incogno creates a hash of the customer name, merchant ID and transaction ID. Thus the customer can choose to identify themselves for dispute resolution, but customer data is not stored in clear text on Incogno servers.

Incogno uses per-merchant pseudonyms generated by a one-way hash of matching first name and last four digits of the credit card number. By using different credit cards, a consumer may choose to have multiple pseudonyms at a single merchant. Incogno is compatible with a large range of personalization services and marketing programs, can track consumer preferences, and, with one pseudonym per customer merchants can provide personalization. The system allows ACID transactions.

Property-Managing Solutions

Figure 3 illustrates the flow of data characteristic of a property-based privacy-protecting technology. Note the user data (represented by the book) remains under the control of the PET provider, as is the case with the seclusion provider.

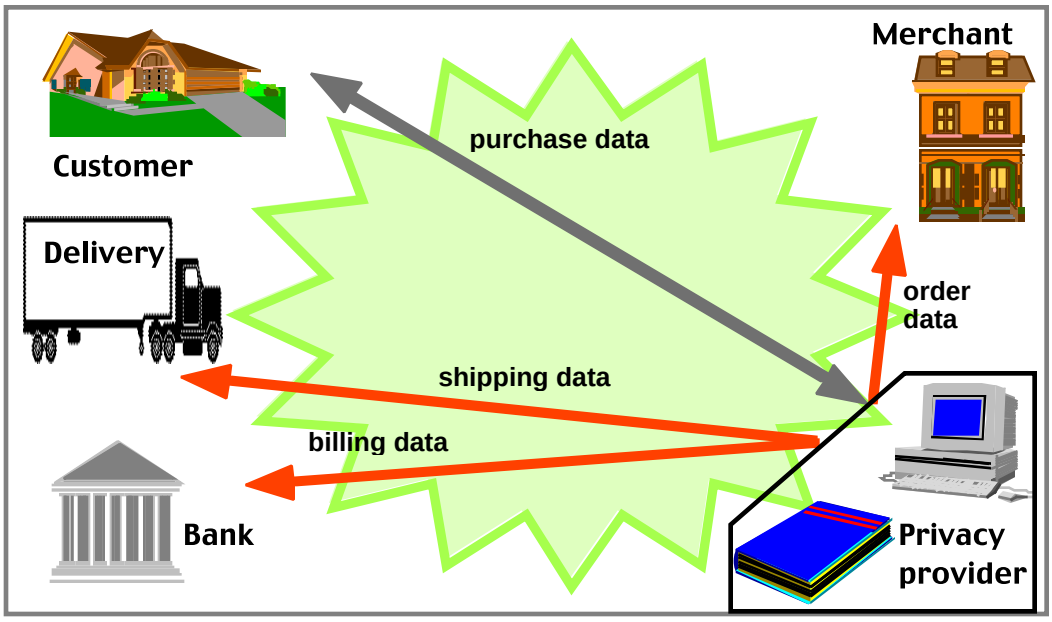

Figure 3: The Data Flow in a Property-Providing Technology

Property exchangers and seclusion providers can be distinguished from other PET providers by two features: location of data and control of data.

First, the location of data stored by the PET provider differs for seclusion-based and property exchange-based technologies. Seclusion providers store adequate data for dispute resolution according to the design of the transactional protocol. Property exchange-based PET providers store detailed data.

Second is the control of data. The seclusion providers allow customers to continue to interact with a merchant based on customer decisions. Incogno allows users to create multiple pseudonyms; Privada and iPrivacy allow users to end associations with specific merchants. With property providers the consumer's control rights are surrendered in exchange for the services provided by the PET. Seclusion customers can choose to provide no data to merchants. With privacy exchanges, the data are owned by service provider and the service provider may track and resell data.

A rough description of the transaction is as follows:

1. Customer obtains software
2. Customer configures software and establishes an account.

3. Encrypted information tunnels through PET provider
4. PET provider distribute data between provider & customer
5. In case of dispute, customer requests data from PET
6. PET resolves dispute, maintains data

With property-based PETs, the user effectively begins by granting agency rights to the privacy provider, which then makes distinct arrangement with merchants for the sharing of data. With seclusion-based PETs, the privacy provider distributes information on a transaction-by-transaction basis, and much data is passed through the privacy provider's without the provider viewing the data.

Microsoft Passport

The Passport service offers a single login service in exchange for consumer data. The consumer provides all data to Passport, and the Passport system audits merchants and controls user data according to merchant/Passport relationships. The concept of privacy, however, is fuzzy and as understood as a good the customer purchases from Microsoft, along with the convenience of one-stop sign-on.

The Passport privacy policy is explicit in its rejection of autonomy. Passport has ownership of all communications and transactional data for any customer or business service or communication. Although its assertion of ownership of intellectual property was modified after customer complaint, Passport retains ownership of transactional data. While Passport is explicit about the privacy policy inside the Microsoft Network, each user is supposed to read and agree with the privacy policy of each affiliated site before any transactions.

The Passport provides two services: identity protection and a wallet. Each user can store his/her credit cards for purchasing activities in the Passport wallet and access them with the single Passport login. The software behind Passport is closed. Transactions are ACID to the extent to which each one of the affiliated companies allows them; meaning that Microsoft will add its transaction-processing services to those of the banks affiliated with the MasterCard and VISA systems.

Passport explicitly sees privacy as a service that can be offered to customers as well as to merchants. The cost to customers is that they have no privacy with respect to Microsoft. Passport is viewed as a mechanism to simplify customer management over data, by removing customer ownership. The high lock-in costs and policies with respect to data ownership illustrate that the system views privacy strictly as a good, and it also views customer data as a good.

Passport confuses the concept of authentication with the concept of privacy. As in the case with iPrivacy, security and privacy are confused. With iPrivacy increased privacy prevents replay attacks. With Passport the concentration of data are presumed to decrease replay attacks and decrease overall consumer risk exposure, as data are not stored in multiple locations across the network.

Conclusions and Future Research

Clearly, the privacy market is either not well understood or parsed by most of the privacy enhancing providers. In general, the security market is confused with the privacy market.

Although security is the control of data while privacy is control of data by the subject, such confusion is in no way inevitable. Specifically, authentication is confused with privacy by the seclusion providers and particularly by Passport. Concentration of data in a third party without subject rights is risk management using an authentication service that does not address privacy.

A significant conclusion is that giving away software is difficult. Even with free or reduced price software, getting users to spend time and extend trust is problematic. Incogno recognized this and targeted privacy-sensitive merchants. iPrivacy seeks to use the pre-existing relationship with card processors in order to connect with consumers. Privada sought to reach customers through the ISP. Yet even these parties had difficulty in getting consumers to install software on their machines.

Network externalities remain a critical source of privacy-enhancing software failure. This presents an ideal opportunity for Microsoft to leverage monopoly power. Unfortunately, the privacy enhancing technology offered by Microsoft through Passport does not actually support privacy as seclusion or autonomy, but rather offers an authentication service which concentrates data.

The seclusion companies offer consumers the ability to reduce their trust in merchants by placing limited trust in the seclusion providers. However, this may be seen as yet another interaction by those wishing to be left alone.

The autonomy providers did well with respect to browsing privacy. Yet the problem of providing privacy in on-line financial transactions remains a practical problem a decade after having been solved in theory. While the autonomy providers may have targeted a more motivated and interested audience, serving the transactional desires remains an unmet goal.

Regarding the comparison across systems, it has been possible to illustrate how different are some alternatives that look very similar (such as Privada, iPrivacy, Incogno and to some extent the Passport). This difference is not only expressed in the types of services offered, but in the assumptions about what "private" information is, who is entitled to its, and in what scope. The PET market can be effectively parsed by using the technological instantiation of the fundamental concepts of privacy.

References

Abric and Kahanês, 1972. The effects of representations and behavior in experimental games. *European Journal of Social Psychology*2:129-144.

Bloustein,, A., 1968. Privacy as an aspect of human dignity: an answer to Dean Prosser. *New York University Law Review* 39:962-970.

Boston Consulting Group, 1997 (March). Summary of Market Survey Results prepared for eTRUST. San Francisco, California: The Boston Consulting Group.

Brands, 2000, *Rethinking Public Key Infrastructures and Digital Certificates : Building in Privacy*, MIT Press, Cambridge, MA.

Branscomb, A., 1994. Who Owns Information? New York, NY: HarperCollins Publishers Inc.

Camp, L.J., 2000,*Trust and Risk in Internet Commerce,* MIT Press, Cambridge, MA

Camp, L.J., 2001, "An atomicity-generating layer for anonymous currencies", *IEEE Transactions on Software Engineering,* Vol. 27, No. 3, pp. 272-278.

Chaum, D., 1988, "Untracable Electronic Cash", *Crypto 88,* Springer-Verlag, Berlin, 319-3127.

Cohen, J., 1996. A Right to Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace. *Connecticut Law Review* 28:981.

Delong, and M. Froomkin, 1997. The Next Economy? in *Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property*, eds. B. Kahin and H. Varian. Cambridge, Massachusetts: MIT Press.

Mell, P., 1996. Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness. *Berkeley Technology Law Journal* 11(1). (http://www.law.berkeley.edu/journals/btlj/index.html.)

Prosser, W.L., 1941. Handbook of the Law of Torts. St. Paul, Minnesota: West Publishing Co.

Rivest, R.L. and Shamir, A., 1996, "PayWord and MicroMint: Two simple micropayment schemes," *Eurocrypt '96*, Springer-Verlag, Berlin.

Shapiro, C. and H. Varian, 1999. *Information Rules.* Cambridge, Massachusetts: Harvard Business School Press.

United Nations, 1995. The United Nations and Human Rights 1945-1995. The United Nations Blue Book Series. Vol. VII. New York, New York: United Nations.

Warren, S. and L. Brandeis, 1890. The right to privacy. *Harvard Law Review* 4:193-220.

Weisband, S. and S. Kiesler, 1996. Self Disclosure on computer forms: Meta-analysis and implications. *Proceedings of the CHI '96 Conference on Human-Computer Interaction*, April 14-22, Vancouver, British Columbia.

Related URLs

Anonymizer
http://www.anonymizer.com/
----. "About Us", Retrieved May 15, 2001, and March 28, 2002.
<http://www.anonymizer.com/corporate/index.shtml>.
----, "Services", http://www.anonymizer.com/privacy_store.shtml, May 15, 2001, and March 28, 2002.
----, "Privacy Policy", http://www.anonymizer.com/docs/privacy_statement.shtml, May 15, 2001, and March 28, 2002.
----, "Terms of use", http://www.anonymizer.com/docs/legal/usage_policy.shtml, May 15, 2001, and March 28, 2002.

Incogno
http://www.incogno.com/)

----, “Privacy statements”, http://www.incogno.com/privacy.html, May 19, 2001.
----, “Frequently Asked Questions”, http://www.incogno.com/faqs.html, May 19, 2001.
----, “Why consumers and merchants need Incogno”,
http://www.incogno.com/incognoResearch.html, May 19, 2001.

Privada
http://www.privada.com/ May 19, 2001.
“Privada Network 3.0 Provides ISP with Solutions for Consumer Privacy”, Press release, http://www.privada.com/news/releases/20010206.html, May 19, 2001.
----, “Individuals”, http://www.privada.com/individuals/index.html,May 19, 2001.
----, “Services”, http://www.privada.com/individuals/services.html, May 19, 2001.
----, “Confidential web browsing” http://www.privada.com/individuals/privadaweb.html, May 19, 2001.
----, “Secure Communication”, http://www.privada.com/individuals/privadamessaging.html, May 19, 2001.
----, “Your Privada Account”, http://www.privada.com/individuals/privadaaccount.html, May 19, 2001.
----“Support”, http://www.privada.com/individuals/support/overview.html, May 19, 2001.
----“Enterprises”, http://www.privada.com/enterprises/index.html, May 19, 2001.

iPrivacy
http://www.iPrivacy.com
----, “This is how iPrivacy works”, http://www.iPrivacy.com/products/iPrivacy.pdf, May 19, 2001.
----, “Consumer privacy policy”, http://www.iPrivacy.com/policy/index.html, March 28, 2002.
----, “Company philosophy”, http://www.iPrivacy.com/stand/ph.html, May 19, 2001.
----, “Press Kit: FAQ”, http://www.iPrivacy.com/press/faq1.html, May 19, 2001
----, “Press Kit: FAQ”, http://www.iPrivacy.com/press/faq.html March 28, 2002.
----, “Protect your privacy”, http://www.iPrivacy.com/protect/index.html, May 19, 2001----, “Protect your privacy”, http://www.iprivacy.com/stand/protect.html, March 28, 2002.

Microsoft Passport
http://www.passport.com/
----, “Privacy Policy”, http://www.passport.com/Consumer/PrivacyPolicy.asp?lc=1033, May 19, 2001, and March 28, 2002.
----, “Business”, http://www.passport.com/Business/Default.asp?lc=1033, May 19, 2001.
----, “Help”, http://memberservices.passport.com/UI/MSRV_UI_Help.ASP, May 19, 2001, and March 28, 2002.
----, “Passport Q&A”, http://www.passport.com/Consumer/ConsumerQA.asp?lc=1033, May 19, 2001 and March 28, 2002.

Zero Knowledge
http://www.zeroknowledge.com/, http://www.freedom.net/ Accessed April 20, 2001.
----, “Freedom ™ Client 2.1. License Agreement” (license agreement displayed in installation executable software)
----, “Freedom Network policies”, http://www.freedom.net/legal-networkpolicy.html?Session=0c4cc2996680805dd6a6bcd84cbdb060, April 20, 2001.
----, “Freedom Network access agreement”, http://www.freedom.net/legal-useragreement.html?Session=0c4cc2996680805dd6a6bcd84cbdb060, April 20, 2001.

----, “Website privacy policy”, http://www.freedom.net/siteprivacy.html?Session=0c4cc2996680805dd6a6bcd84cbdb060, April the 20th, 2001.
----, “Website privacy policy”, http://www.freedom.net/siteprivacy.html?product=suite March 27, 2002.
----, Freedom Internet Privacy Suite 2.0, http://www.freedom.net/info/index.html?Session=fbf49f6af59aaba0fb88219fd1e09dae
----, Back, A., I. Goldberg, and A. Shostack. “Freedom 2.0 security issues and analysis.” Nov. 2000. <http://www.freedom.net/info/whitepapers/Freedom_Security2-1.pdf?Session=fbf49f6af59aaba0fb88219fd1e09dae>
----, Boucher, P., A. Shostack,. and I. Goldberg. "Freedom Systems 2.0 Architecture." Dec. 2000. http://www.freedom.net/info/whitepapers/Freedom_System_2_Architecture.pdf?Session=fbf49f6af59aaba0fb88219fd1e09dae
----, Samuels, R. and E. Hawco, “Untraceable nym creation on the Freedom 2.0 network.” Nov. 2000. <http://www.freedom.net/info/whitepapers/Freedom-NymCreation.pdf?Session=fbf49f6af59aaba0fb88219fd1e09dae>
----, “Private credentials“, Nov. 2000, http://www.freedom.net/info/whitepapers/credsnew.pdf?Session=fbf49f6af59aaba0fb88219fd1e09dae
----, “Private sector: the newsletter of privacy and enterprise 1.1”, Nov. 2000, http://privacy.zeroknowledge.com/publications/pdf/privatesector1-1Nov2000.pdf
----, “Private sector: the newsletter of privacy and enterprise 2.1”, Mar. 2001, http://privacy.zeroknowledge.com/publications/pdf/privatesector2-1Mar2001.pdf