

A new framework for the analysis of solutions for privacy-enhanced Internet commerce

Carlos A. Osorio¹

carlos_osorio@ksg01.harvard.edu

Abstract -- In order to examine the emerging market for privacy-enhancing service in Internet commerce it is critical to examine the relationship between privacy, security, and commerce. In order to function, a privacy-protecting technology must have a coherent trust model, a sustainable business plan, and a solid design for security. Yet, the sustainability of business plans can vary across regulatory regimes and concepts of privacy vary between cultures. Furthermore, privacy can be understood as a right of property, autonomy or seclusion.

This paper presents a new framework to assess the suitability and effectiveness of business approaches to privacy and tests it analyzing six well-known systems: Zero Knowledge, Incogno SafeZone, Privada Control, iPrivacy, Passport, and the Anonymizer. We have specifically chosen not to examine smart-card based approaches, such as the American Express Blue.

Each system is examined based on its underlying conception of privacy (seclusion, autonomy, property); ACID characteristics (atomicity, consistency, isolation and durability); general business plan; consumer switching cost; availability or openness of software; usability and accessibility.

This paper argues that these elements together illustrate the economic, privacy, and security implications of any one system. The analyzes can encompass the context generated by bias and ontology in the solution and the way in which -by the interaction of its technological and business dimensions- it creates realities, rule-setting and reaches minimum standards of integrity, nonrepudiation, confidentiality, reliability, authentication and security in their search for privacy.

This work presents the framework, apply it to well-known systems, and offers the results not only as an examination of the privacy-enhancing commerce systems themselves, but also as an implicit commentary on the value of the framework developed.

The framework: an overview

Osorio (2001) discuss the way in which technologies are designed as representations of new or improved realities in order to accomplish an objective. Thus, technological

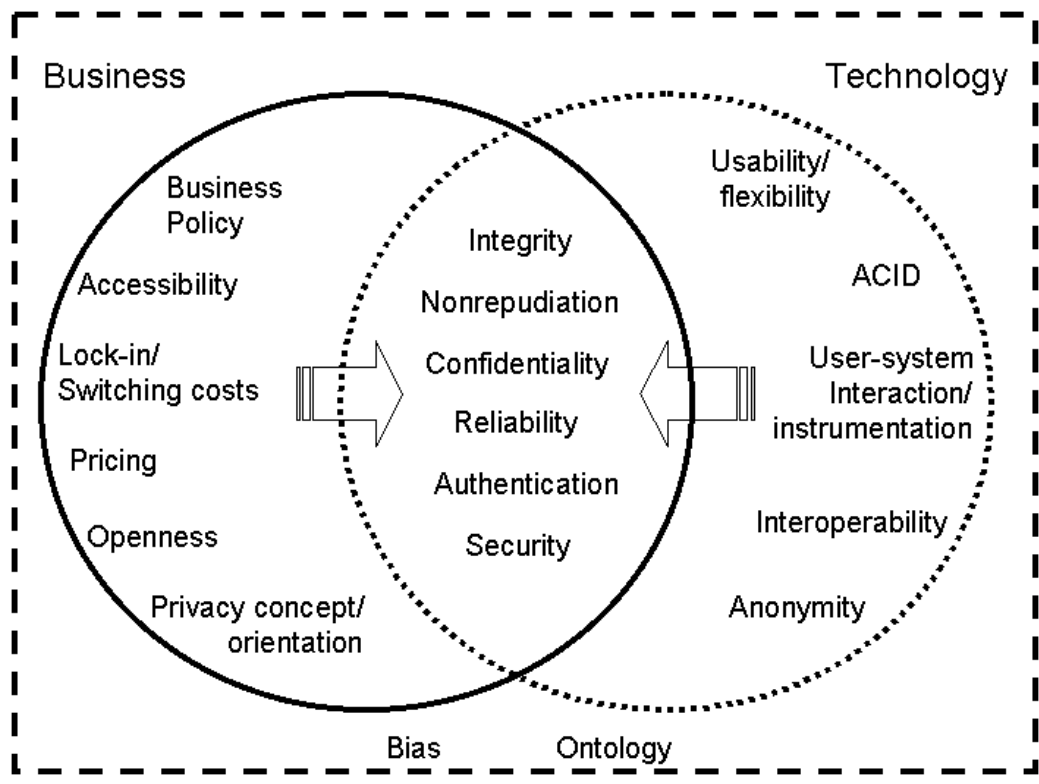
¹ Carlos A. Osorio is Research Associate at the Information Technologies Group at Harvard University's Center for International Development, and Visiting Scientist at MIT Media Lab. I appreciate the comments and suggestions of Prof. Jean Camp, from Harvard University's John F. Kennedy School of Government. I, however, remain the sole responsible for any errors.

solutions can “create” realities by which one is able to freeze and save a moment in a picture. Information technologies and, in particular, privacy-enhancing solutions for electronic commerce respond to this reality. Privacy is an inherently social characteristic that, as suggested by Camp (2000), can be understood as property (good), autonomy (right) or seclusion (state).

Privacy-enhancing solutions for e-commerce are mechanisms intended to create or represent a desired reality about what privacy should mean, how it should be treated and protected. They are the result of the interaction between a specific bias toward it, and a determined ontology about how privacy should be provided. This bias and ontology, therefore, are embedded in the design of these solutions’ business plan and a technological model.

Thus, the technological model or representation -Lessig’s code- creates a new reality through a set of rules. By the other hand, a special bias about the meaning of privacy (as good, state or right) generates the basis for a respective business plan that, sometimes, counteracts with the technological model. This interaction is represented in Figure 1.

Figure 1: Alignment of dimensions for analyzing privacy-enhancing technologies



Source: Osorio (2001)

The figure illustrates the core of the framework. The roles of bias and ontology have been explained. There are two major dimensions: the technological and business models, which respond to different incentives in a same social embeddedness (a technically feasible solution, in the first, and an economically profitable one in the second.) These

two dimensions interact and should meet minimum socially accepted standards of integrity, nonrepudiation, confidentiality, reliability, authentication and security in order to offer a privacy-enhanced service or solution for electronic commerce.

In looking for these characteristics, the effect of the business dimension is the result of definitions on business policy about privacy, accessibility to personal information, the system's generation of lock-in and cost of switching, openness, adoption of a determined privacy concept and, related to it, a pricing method to value privacy. Interacting with it, the technological dimension considers the levels of anonymity that can be obtained by using the solution; the atomicity, consistency, isolation and durability of commercial transactions (ACID property); and usability. Other two technical dimensions are the solution instrumentation and interoperability².

Applying the framework

In this section, we apply the framework to the analysis of ZeroKnowledge's Freedom Internet Privacy Suite 2.0, Privada Control, iPrivacy, Anonymizer, Microsoft Passport and Incogno SafeZone³.

Analyzing the privacy-enhancing solutions

The study of different solutions has shown great consistency between the principles stated in the company's mission, their definition of privacy, and the bias and ontology embedded in the solution.

✍ **ZeroKnowledge (ZNK):** The Company is biased pro open source software, which can be appreciated by the large amount of information and resources available about the solution. Privacy is understood as seclusion and the solution is defined as a technological approach to solve a problem that policy won't do: protect privacy by generating a pseudonym system, where a user can buy different "nyms" that have limited duration. While privacy is defined as seclusion in the relationship between the customer and the world, which is possible by the technological model, it is treated as property and autonomy between the company and the user (as result of the business model). It is possible to have free access to the software, which allows limited levels of privacy and quality of service, but if the client wants to have "the right to be let alone" and be autonomous, he or she has to pay \$49.95 by five pseudonyms per year. The system is relatively easy to use, with low switching costs, and very interoperable, which is consistent with ZNK's principles. Transactions have ACID properties.

✍ **Privada Control:** Privada considers privacy as primarily autonomy and, as such, it directs its solution to ISP and companies. This approach, plus a bias toward technologically regulated environments, generated a solution in which Privada creates a secure virtual private network (Privada Network) with its business clients, which can offer the client software for their respective clients. Privada does not charge users, and makes them easy to operate the software putting the burden in the companies' hands. The business plan, however, may generate great switching costs

² See Osorio (2001) for a more detailed analysis.

³ See tables 2, 3, 4, 5, 6 and 7, respectively, at the annex.

for the users if, for instance, an ISP does not allow interoperability with other privacy solution. In a case like this, the only possibility is to change ISP, which requires change in email, a feature with important lock-in and relatively high associated switching costs (this would also happen in the case of the customer's credit card company). While privacy is understood as autonomy in the technological model, its interaction with the business model generate lock-in and costs high enough to diminish autonomous behavior among the people more sensible to privacy. ACID properties of transactions depend of each affiliated company.

✍️ **iPrivacy**: For iPrivacy, the Internet should be as private as in the offline World. Privacy is understood as autonomy for the people and, in order to provide it, the solution is licensed for credit card and shipping companies disintegrating the merchant of the information supply chain. Here, the system generates encrypted data for the merchant and shipping companies, so each one knows the minimum pertinent personal information required for performing its activities. With a transaction-oriented approach, the system does not provide anonymity, but privacy as in the offline world. Thus, the credit card company always has access to all information. As in Privada Control, iPrivacy generates high lock-in and switching cost associated in the event a credit card company decides to make the system its way of doing business online. It may be easier to change software than change a credit card. Transactions have ACID properties.

✍️ **Anonymizer**: Considers privacy as solitude (for all except purchasing) and provides a system that generates privacy and anonymity by two approaches. First, it provides a web-based environment where the system becomes a firewall between the user and third parties, mirroring the Internet content requested by the customer and hiding his or her identity to third parties. Second, it provides software-based solutions to manage security at the PC level and provide additional security features to its web-based services. The idea is to let the user alone on his/her Internet experience. Its pricing model, however, treat privacy as a good that can be supplied regarding each user's privacy-sensitivity and willingness to pay. Thus, its services have different prices depending of their privacy-enhancing characteristics, and are bundled in completeness, creating increasing lock-in with price (i.e. privacy is treated as property). It does not guarantee ACID transactions. These properties are function of each merchant check-out, shipping systems and policy.

✍️ **Microsoft Passport**: The passport ontology is that of a private network that can guarantee a person "security" in purchasing activities. The passport creates a system that, if the user decides, provides anonymity with respect to those outside the network and the transaction. The concept of privacy, however, is fuzzy and is understood as a right the customer share each time he or she purchases. 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 making transactions with it. The Passport provides two services: identity protection and a wallet, in which each customer can store his/her credit cards for purchasing activities. The system is free. There is an important reason for this, which explains part of the bias of this

solution, is Microsoft's desire to increase the value of its network by generating a standard for payment across sites and increase the value and use of Microsoft online services (Which is consistent with using a easy-to-use and relatively open solution). Transactions are ACID to the extent to which each one of the affiliated companies allows them.

✍ ***Ancogno SafeZone***: This is a patent-pending solution. It considers private information as property, and recognizes its value in the business process. Thus, SafeZone allows merchants to tailor de levels of privacy they want to provide to their customers. Thus, Incogno serves as a trusted third-party that manages the relationships between the credit card company, the merchant and the shipping company, restricting the information the merchant decides to do not collect from its customers. The relation with the customers is managed as if privacy were a mix between autonomy and solitude: while the system work as a traditional check-out, but it's trusted and varies across merchants. The company, however, declares that Incogno is compatible with a complete range of personalization services and marketing programs, still can track consumer preferences, and by matching first name and hour last digits of the credit card, the merchants can establish a person status as customer. The system allows ACID transactions.

Table 1: Characteristics of privacy across solutions

	ZeroKnowledge	Privada	iPrivacy	Anonymizer	Passport	Incogno
Business concept of privacy	Property/Autonomy	Autonomy (little)	Autonomy	Property	Varies	Property
Technological concept of privacy	Seclusion	Autonomy	Autonomy	Seclusion	Autonomy	Seclusion
Pricing	Varies across services	Free to people. Licensed to companies	Free to customers. Solution is licensed to companies	Varying across products and bundles	Free	Free to people. Charge merchants
Security	Yes	Depends of each affiliated company	Yes	For all except purchasing	Depends of each site	Depends of each merchant
Integrity	Yes	Depends of each affiliated company	Yes	For all except purchasing	Varying across affiliated sites	Yes
Nonrepudiation	Yes	Depends of each affiliated company	Yes	No	Yes	Yes
Confidentiality	It is possible using digital cash	Depends of each affiliated company	Not higher than in the offline world	For all except purchasing	Only outside the Passport network	Each merchant decides
Reliability	Yes	Yes, only among affiliated	Yes	For all except purchasing	Yes	Yes
Authentication	Yes	Yes, function of each affiliated companay	Yes	No	No	Yes

Source: the author's analysis considering companies' information

As illustrated by Table 1, the effect of each alternative varies across solutions and, with the sole exception of iPrivacy, the perceived concept of privacy used in the technological model is different than in the business model. One major issue that can be identified from this analysis, and is relevant to the effectiveness of each solution, is the extent to which the interaction between bias, ontology, business and technological model define the scope of privacy.

Regardless what of the definitions of privacy is used (property, autonomy or seclusion), understanding the scope in which privacy is defined is crucial in defining the overall effectiveness of the solution, and the coherence between its technological and business models. Thus, it is possible to see how companies that focus privacy in the individual tend to (1) provide a user-focused service, or (2) do not provide privacy services centered in Internet-based purchasing (ZeroKnowledge and Anonymizer, respectively). By the other hand; iPrivacy, Privada, Passport and Incogno assume privacy in a scope that goes beyond the user, or assume the user autonomy to go beyond his or her own scope. In this context, iPrivacy looks as the most coherent solution by equalizing privacy between the online and offline world. In this context, it is interesting to see the way in which Microsoft and Incogno inherently recognize that merchants have a right to people's information.

Thus, while almost all solutions provide privacy protection against "unauthorized third-parties", the changing definition of what an "unauthorized third-party" is generates that - with the sole exception of ZeroKnowledge- the analyzed solutions provide options for secure online payment, instead of a totally private online buying experience, windows shopping included.

Discussing the framework

As illustrated in the previous discussion and each alternative's table at the annex, the framework provides a method to analyze the coherence and overall impact of privacy-enhancing services for Internet commerce. The challenges in meeting with the characteristics of privacy can be appreciated in Table 1, where is possible to see how also in privacy "there is no such a thing as a free lunch". When the solution is free, it is being licensed to companies and then security and confidentiality are constrained by each merchant's, or authorized third-party's, policy.

A privacy-protecting technology must have a coherent trust model, a sustainable business plan, and a solid design for security, which are interacting features closely related with the definition and scope of privacy. As analyzed, the framework gives importance to identify the bias and ontology employed in the definition of privacy, its scope, the design of the trust model, the business plan and the resulting design of security.

In this context, the separation of the analysis in (1) interaction between the individual and the solution, (2) its interoperability with other systems and third-parties, and (3) features in online shopping are important to disaggregate how privacy is considered across relationships and analyze the differences in accessibility, lock-in and switching costs, degrees of openness, anonymity, usability, pricing and ACID properties.

Privacy needs to be defined in a determined way to create a technological solution that is feasible and approaches the privacy issue from a perspective of solution-seeking. This is obtained by privacy's relevance in the creation of, and coherence between, the trusted model and security design. Here, the identification of the privacy concept, and analysis of usability, characteristics for ACID transactions, interoperability and anonymity play a critical role.

By the other hand, the business model represents the roadmap by which the solution will reach economic feasibility and long-term sustainability. Here, the framework also identifies the privacy concept assumed in the business model; its policy related to interaction with the customer, third-parties and in shopping activities (if offered); the generation of lock-in and switching costs, and the definition -with important effects in the technological solution- of degrees of openness and accessibility.

Conclusions and directions for future research

This paper's objectives were to present the framework developed in Osorio (2001), applied it to well-known privacy-enhancing solutions and assess its own value as methodology of analysis.

Regarding the comparison across systems, it has been possible to illustrate the differences of some alternatives that may look very similar (such as Privada, iPrivacy, Icogno and, to some extent, Microsoft 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 it, and in what scopes. Thus, it has been possible to see how these aspects affect the quality of different trusted models. Also, the analysis allows the identification of those solutions that offer secure, but not private in an absolute sense, transactions. In this context, it has also been possible to illustrate the relevance of the coherence between the privacy concepts used in the technological and business models in the creation of a solution that provides the services it intends to.

In terms of the analyzed solutions, two of them (ZeroKnowledge (ZKS) and the Anonymizer) are focused in the individual. Both consider privacy as seclusion in the technological models, while the business concept of privacy for ZKS is a mix between property and autonomy, and for the Anonymizer is property. The major difference is that ZKS considers privacy as an absolute concept in which the subject generator of information -the person- is the only with rights to decide about that information.

From these solutions, iPrivacy approach deserves special attention by the coherence between the technological and business models. The ontology is extremely logic and considers the effect of social and organizational embeddedness of persons and companies by equalizing the online and offline world. There is an assumption about requirements of safety, security and risk-taking for both companies and people that is natural in the offline world and the solution tends to replicate it online. The solution only provides real identity information for credit card and shipping companies, making extremely difficult the use personal information for merchants (as in the real world).

It is possible to conclude the only systems that, one would say, really provide a private solution for electronic commerce, in the sense defined by them, are ZeroKnowledge and iPrivacy. See Table 1 and appreciate that confidentiality can be reach in the first option by using digital cash and, in the second, is constrained by the company's concept of privacy⁴.

⁴ As suggested by Camp (2001), it is possible to have an anonymous system that offers reliable transaction.

The framework proved to be of great utility in examining these alternatives. It provides a method to analyze the way in which privacy-enhancing solutions operate in terms of their interaction with the person, how they interoperate with different systems, and how they work while conducting online purchasing. The approach of considering bias, ontology and the variation of the privacy concept shown to be adequate to understand the different effects of lack of coherence between the technological and business models.

A special comment, important for future research, deserves the six characteristics of privacy. While the results of the analysis of the selected privacy-enhancing alternatives is a good indicator about the goodness of the framework, it would be desirable to consider a larger number of alternatives, especially focused into the person, and analyze how integrity, nonrepudiation, confidentiality, reliability, authentication and security works in generating a private system. Additional analysis would be especially interesting in identifying features that have not been considered in the development of privacy-enhancing services for Internet Commerce, or the major differences in the technological design and business models between B2C and B2B-oriented solutions.

< Tables 2, 3, 4, 5, 6 and 7 here >

References

1. Anonymizer, <http://www.anonymizer.com/> (Accessed on May 1, 2001)
2. ----, "About Us", <http://www.anonymizer.com/corporate/index.shtml>
3. ----, "Services", http://www.anonymizer.com/privacy_store.shtml
4. ----, "Privacy Policy", http://www.anonymizer.com/docs/privacy_statement.shtml
5. ----, "Terms of use", http://www.anonymizer.com/docs/legal/usage_policy.shtml
6. Camp, L. J. (2001) "An atomicity-generating protocol for anonymous currencies", IEEE Transactions on Software Engineering, Vol. 27, No.3, March 2001.
7. Osorio, C. (2001) "Dimensions for the analysis of privacy-enhancing solutions for electronic commerce", Working paper, John F. Kennedy School of Government, Harvard University, May.
8. Incogno, (<http://www.incogno.com/> accessed on May 15, 2001)
9. ----, "Privacy statements"
10. ----, "Frequently Asked Questions"
11. Privada, <http://www.privada.com/> (Accessed on May 10, 2001)
12. "Privada Network 3.0 Provides ISP with Solutions for Consumer Privacy", Press release, <http://www.privada.com/news/releases/20010206.html> (Accessed on May 10, 2001)
13. ----, "Individuals"
14. ----, "Services"
15. ----, "Confidential web browsing"
16. ----, "Secure Communication"
17. ----, "Your Privada Account"
18. ---- "Support"
19. ---- "Enterprises"

20. iPrivacy, <http://www.iprivacy.com> (Accessed on May 10th, 2001)
21. ----, "This is how iprivacy works", <http://www.iprivacy.com/products/iprivacy.pdf>
22. ----, "Consumer privacy policy", <http://www.iprivacy.com/policy/index.html>
23. ----, "Company philosophy", <http://www.iprivacy.com/stand/ph.html>
24. ----, "Press Kit: FAQ", <http://www.iprivacy.com/press/faq1.html>
25. ----, "Protect your privacy", <http://www.iprivacy.com/protect/index.html>
26. Microsoft Passport, <http://www.passport.com/> (Accessed on May 5, 2001)
27. ----, "Privacy Policy",
<http://www.passport.com/Consumer/PrivacyPolicy.asp?lc=1033>
28. ----, "Business", <http://www.passport.com/Business/Default.asp?lc=1033>
29. ----, "Help", http://memberservices.passport.com/UI/MSRV_UI_Help.ASP
30. ----, "Passport Q&A",
<http://www.passport.com/Consumer/ConsumerQA.asp?lc=1033>
31. Zeroknowledge, <http://www.zeroknowledge.com/>, <http://www.freedom.net/>
(Accessed in April 4, 2001)
32. ----, "Freedom™ Client 2.1. License Agreement"
33. ----, "Freedom Network policies"
34. ----, "Freedom Network access agreement"
35. ----, "Website privacy policy"
36. ----, Freedom Internet Privacy Suite 2.0,
<http://www.freedom.net/info/index.html?Session=fbf49f6af59aaba0fb88219fd1e09dae>
37. ----, "website privacy policy",
<http://www.freedom.net/siteprivacy.html?Session=fbf49f6af59aaba0fb88219fd1e09dae>
38. ----, "Untraceable nym creation on the Freedom 2.0 network", by Samuels, R., and Hawco, E., Nov. 2000, <http://www.freedom.net/info/whitepapers/Freedom-NymCreation.pdf?Session=fbf49f6af59aaba0fb88219fd1e09dae>
39. ----, "Freedom 2.0 security issues and analysis", by Back, A., Goldberg, I., and Shostack, A. Nov. 2000,
http://www.freedom.net/info/whitepapers/Freedom_Security2-1.pdf?Session=fbf49f6af59aaba0fb88219fd1e09dae
40. ----, "Private credentials", Nov. 2000,
<http://www.freedom.net/info/whitepapers/credsnew.pdf?Session=fbf49f6af59aaba0fb88219fd1e09dae>
41. ----, "Freedom Systems 2.0 Architecture." by Boucher, P. Shostack, A. and Goldberg, I. Dec. 2000,
http://www.freedom.net/info/whitepapers/Freedom_System_2_Architecture.pdf?Session=fbf49f6af59aaba0fb88219fd1e09dae
42. ----, "Private sector: the newsletter of privacy and enterprise 1.1", Nov. 2000,
<http://privacy.zeroknowledge.com/publications/pdf/privatesector1-1Nov2000.pdf>
43. ----, "Private sector: the newsletter of privacy and enterprise 2.1", Mar. 2001,
<http://privacy.zeroknowledge.com/publications/pdf/privatesector2-1Mar2001.pdf>