

“The Privacy Paradox”

Minas Samatas
Sociology Department
University of Crete
samatas@social.soc.uoc.gr

1. Privacy concerns and 'the privacy paradox' for web users

As it is documented by several online or internet privacy surveys, web users place privacy high on their list of concerns, yet they take few voluntary steps to protect it. Most Web users become more pragmatic.

Thus, while most Internet users express high privacy concerns, when asked in general terms and overwhelmingly want the presumption of privacy when they go online, in practice a great many of them do nothing or little to protect it. Either they do not know the basics of how their web activity is observed and how to use available tools to protect themselves, or feel weak to defend themselves against intrusive practices. Because of that, many resist to provide personal information, and others take risks and exchange their privacy for some benefits. At the same time despite their concerns, many Web users do a striking number of intimate and trusting things on the Internet, like personal chat rooms, online dating, etc.; they also use “guerrilla tactics” providing a fake name or personal information to defend their online privacy.

(see : AT&T Labs Research Technical Report “Beyond Concern: Understanding Net Users’ Attitudes about online Privacy” 1999; the Pew Internet & American Life Project “Trust and Privacy online: Why Americans Want to Rewrite the Rules”, August 2000; and Information Technology Association of America (ITAA) Industry Pulse Electronic Commerce Barriers Survey, 2002).

- **A typology of Internet users' privacy concern**

The vast majority of online consumers are more pragmatic regarding online privacy.

According to the findings of a 2002 e-mail survey on privacy concerns of Internet users, while in offline environment only ¼ of consumers are highly concerned about privacy, ¼ are not concerned and half are pragmatic, in that their privacy concerns depends on situation presented, the vast majority of online consumers are more pragmatic regarding online privacy . High levels of education are more concerned than those with less education; persons over the age of 45 tended to be either not at all or enough concerned. Younger persons tended to be more pragmatic. (Kim Sheehan,*The Information Soc.* **18(1) 2002**).

What do these pragmatic attitudes actually mean ? do they mean that state and corporate privacy violations and coercive surveillance becomes routinized and taken by the Web users for granted?

- **Public privacy concerns suggest that the state and business organizations are failing to gain Web users trust.**

The public's non-volatile and growing **concern about privacy**, particularly in relations to electronic commerce and interactive media systems, appear to suggest that state and business organizations are failing to gain trust and indeed are engaging in practices that lead to mistrust among web users. Analysts estimate that Internet retail sales lost due to **privacy concerns** may be as much as \$18 billion (Gellman R. 2000).

Those Web users who attempt to protect their privacy proactively are often thwarted by a "web" of obstacles: governmental security requirements favouring states' ease of access versus individual privacy rights; widespread use of online profiling - customer information profiles for marketing via conventional and Internet channels; and the prevalence of profitable "dataveillance," "spyware," as well as other illicit web surveillance enterprises.

2. The contrast of Privacy as a human right-value vs privacy as an economic right and commodity

- **Privacy is a shifting and a contentious notion, and a value – laden concept, and it is hard to reach consensus on a definition.**

The U.S. economic-technological privacy approach , that is privacy as an economic right, stands in direct contrast to the European social values – oriented assertion of privacy as a human right.

An intermediate concept is that of (information) **privacy as an interest**, rather than as a right, i.e., “the interest individuals have in controlling, or at least significantly influencing, the handling of data about themselves.” An interesting implication of the definition of privacy as an interest is that it has to be balanced against many other, often competing, interests.

Hence, **privacy protection** is a process of finding appropriate balance between privacy and multiple competing interests., e.g. law & order (Clarke R. 2000).

- **Privacy as a commodity and the growing privacy market in information capitalism.**

In information capitalism: **high-tech surveillance** is already a structural feature of political and corporate power (Castels M. 1996, Giddens A. 1990); and **information privacy protection produces a market where privacy is no longer a right but a commodity, available only to those who can afford it.** So, lack of privacy protections in the privacy market arena there is a privacy toll measured in dollars and in hours (Gellman R. 2000).

Non-economic interests protected by privacy policy and laws, like the exercise of freedom of expression , the protection of children, cannot be measured in dollars.

The danger of this trend of privacy commodification will add yet another dimension to the stratification ladder in society by privileging the educated and those who possess the means to transact in the information marketplace, leaving by the side the poor, uneducated, and the unskilled.

Unless privacy is asserted as a human right with substantial protections for all individuals, the increasing trust distance between individuals and institutions will may result in the breakdown of social and economic processes.

3. The primacy of security and the reduction of privacy to data security

The proponents of security and e-commerce bind trust and privacy too closely to security; they diminish the rich , complex, intensely social , cultural and moral concept of trust and privacy for merely one slim part of them (Nissenbaum 2001).

From the security point of view, privacy is a value rather than a right, which imperils efficiency and shields criminals and terrorists. It is a natural enemy of freedom of information. Its enforcement is cumbersome and expensive (Davies 1997:153).

Long before the September 11, there is a shift **from privacy protection to data protection or data security**. Yet, this trend especially the last two years after the **September 11**, is intensified.

4. Every Privacy protection is still insufficient

Privacy protection either entirely through technology or entirely through law, or protection through a combination of law and technology are proved to be insufficient (Clarke R.2000)

- European Privacy protection legislation is insufficient. Data protection acts and institutions generally have serious limitations; they are not privacy laws but information laws protecting data before people.
- American-style self-regulation and optional privacy seals are widely considered ineffective .
- Furthermore, individualistic "informational self-determination," which leaves web users to make decisions on which data they consent to make available, and in which instances they refuse its availability, is impractical.
- **Information Security is not panacea**

Can privacy be secured online by firewalls, biometrics, digital signatures, intrusion detection, auditing? **Security is not panacea;** it is not bringing about trust. **Powerful security mechanisms may keep us safe from malicious individuals but not from agents and institutions.** The important barriers to trust online are not only the evil hackers, but “ **the conditions of imbalance between individual and institutions.** ” (DiMaggio et.al. 2001).

5 . The significance of Trust

- Trust , both in persons and systems, has strong aspects of mutuality. Privacy is a precondition for trust and trust affects privacy. The resultant spiral will lead to stable and productive relationships.
- Trust facilitates web users to risk their privacy, but they are still vulnerable. Trust in the adequacy of privacy-protection legislation and privacy "hard" systems is a significant "soft" factor for information quality and ICT-based information systems.
- **Internet trust, not just as a technological or security issue, but as a multilateral socio-psychological relationship demands more cooperative interactions.**

6. **From individualistic privacy concerns to the state & corporate power & surveillance concerns.**

- The asymmetry of Individual privacy vis a vis state and corporate power.

Internet dramatically shifts the balance of power between Web users and Web providers, business and customers . Now this balance is against users and consumers; however in the long run, because the Web offers unprecedented opportunities for interacting , the most effective way for Web providers to develop successful exchange relationships with online users is to gain their trust by allowing the balance of power to shift toward more cooperative interactions between providers and users.

7. Reconsidering the right of Privacy

- **Rethinking privacy and trust from not only the viewpoint of the consumer and commerce, but all internet users , citizens , the system designers or the policy makers.**
- **We have to see the privacy and trust problem not as an individual and personal issue, but as a part of a new landscape of social power, in order to limit the concentration of state and corporate power in our democracies, to enhance the power of people as citizens, consumers and Web users in general .**
- start demand accountability of those whose power is enhanced by unchecked surveillance and privacy intrusions.
- In information-capitalist democracies there must be mechanisms to enforce institutional accountability, and "top-down" punishment for all privacy violators . Furthermore, consumer unions, privacy rights and other interest groups should be vigilant in identifying and exposing privacy violators, boycotting and taking effective action from below.

8. **Solution : Information security or / and Information trust culture based on information ethics and promoted through responsible computing.**

- **computer security is a Sisyphusian battle due to the ‘open’ architecture and permissive nature of the Internet and Web .**

No matter what laws are passed, and how good security measures might become, they will not be enough for us to have completely secure systems. We also need **to develop and act according to some shared ethical values** & enhancing privacy and trust through **responsible computing** i.e., computer training **with values**.