Managing IS Security and Privacy

Vasilios Katos
University of Portsmouth, UK

INTRODUCTION

The concept of privacy has received attention for over a century now and its definition—let alone, understanding—has been profoundly challenging. This is primarily attributed to the "incompatible" and rich set of characteristics privacy comprises. As Brunk (2002) states very sharply, "Privacy is a matter of intellectual and philosophical thought and retains few tangible characteristics, making it resistant to simple explanation."

Perhaps the first scholarly work on privacy was that of Warren and Brandeis (1980), who introduced the highly abstractive yet popular definition of privacy as the "right to be left alone." As privacy was recognized as a right, it primarily existed within a legal context. Legislation for protecting one's privacy exists in many countries and in some cases at a constitutional level (see for example the Fourth Amendment of the U.S. Constitution).

It was soon realized in the information revolution era that privacy and information are somewhat coupled. More precisely, emerging privacy concepts and metrics relate to the intentional or unintentional information flows. However, when it comes to studying, using, and investing in information, security appeared to have a higher priority over privacy. Security and privacy seemingly operate under different agendas; privacy is about protecting one's actions in terms of offering anonymity, whereas security includes the notion of accountability which implies that anonymity is waived. Still, security is a vital component of an information system, as it is well needed in order to protect privacy.

This contradictory relation between security and privacy has caused a considerable amount of debate, political and technical, resulting in a plethora of position and research papers. Accepting that there may be no optimum solution to the problem of striking a balance between security and privacy, this article presents a recently developed methodology that could support policy decision making on a strategic level, thus allowing planners to macro-manage security and privacy.

BACKGROUND

A thorough overview on the economics of privacy is maintained by Acquisti (2008). The 1970s was a decade marked by economists and their aspirations to develop an economic model to "decrypt" the market forces. Although Hirshleifer (1971) introduced the value of information in relation to privacy in the early 1970s, economics tools were ported to the privacy domain in the late 1970s and early 1980s (e.g., Posner, 1978; Stigler, 1980). However in the 1980s the concept of information sharing and the Internet were showing signs of potential, only to be interrupted by the Morris Worm in 1988 (Seeley, 1989), and security was added into the agenda. Initially this was done in the expense of privacy. For the following years information security received substantial attention—if the members of the private sector were to invest in electronic communications and technologies, trust needed to be restored.

Formal treatment of information security was initially in the domain of cryptography, but soon expanded to access control models and intrusion detection systems. The security goals of confidentiality, integrity, and availability were defined. The escape from security being equivalent to confidentiality was soon realized in the domain of cryptography, which was enforced with Rivest's (1990) definition of cryptography which "is about communication in the presence of adversaries." As such, the adversary would not necessarily be interested in eavesdropping on a communication, but could elect to interrupt, modify, fabricate, or replay messages. Formally, this omnipotent adversary was initially captured in Dolev and Yao's (1981) threat model, spawning research into cryptographic protocols.

To date, the body of knowledge for information security has fairly matured. The security domains include both technical and organizational aspects. Standards and methodologies emerged—see for example BS 7799 and ISO/IEC 17799 (BSI, 1995a, 1995b), ISO 27001 (ISO, 2005, aligning with BS 7799 part 3), and CobiT (IT Governance Institute, 2007). It can be seen from the directions taken by these standardization efforts that information security management was becoming an isomorphism of risk management: understanding that there is no absolute security, controls need to be in place in order to diversify the risks of unauthorized disclosure (breach of confidentiality), unauthorized modification (breach of integrity), and denial of service (breach of availability), accepting that there is an amount of residual risk that will be present after employing the security controls.

Research on privacy followed at a much slower pace. It could be argued that a valid reason for this is that privacy is upper bounded by security; security needs to be in place in order to offer privacy. Indeed, some security technologies

such as cryptography were branded as privacy enhancing technologies (PETs), emphasizing the synergetic relationship between security and privacy. As the number of privacy violations and intrusions was steadily increasing in the 1990s (Acquisti, 2008), research on privacy gained momentum. Similar to the security goals stated earlier, the privacy criteria of unobservability, pseudonymity, unlinkability, and anonymity (ISO, 1999; Fischer, 2001) were introduced. With respect to the economics of privacy, the work by Laudon (1996), Varian (1996), Huang (1998), and Posner (1999) set precedence leading to research in the formal application of micro-economic techniques to analyzing privacy. Representative work on the formal application of micro-economics on privacy was published by Acquisti (2004; Acquisti, Dingledine, & Syverson, 2003), Otsuka and Onozawa (2001), and Ward (2001).

However, it was realized by Katos and Patel (2008) that a micro treatment of privacy would be applicable in establishing operational management procedures, yet it had major limitations when attempting to understand the challenges in balancing security and privacy when engaging in policy-making activities. The authors argued that a detailed (micro) view of privacy and security would make it virtually impossible to track or predict the outcome of a policy decision, and suggested that a higher-level—or aggregate—view should be adopted. In fact, Odlyzko (2003) conjectured that the privacy problem is intractable. An analogy could be drawn with the stock market environment: although trends could be established on a macro level for the performance of a certain market, the actual assessment and prediction of the micro variables (stocks) would be substantially more challenging, error prone, and less informing.

The following section presents a methodology developed as a response to the shortcomings of the micro views on security and privacy. The section summarizes the main points of the model. For a more detailed explanation, the reader is referred to Katos and Patel (2008).

A MACRO TREATMENT OF INFORMATION SECURITY AND PRIVACY

Initially we accept that there is no universally accepted, objective measure for privacy. As privacy applies not only to the data, but also to the user's actions as he or she interacts with any given system, we can consider a space of events that could be expressed by a set as follows:

$$A=\{stay\_home, go\_shopping, use\_credit\_card, mortgage\_application, \ldots\}$$

If a metric $p(\ )$ on privacy existed, mapping the above set into a formal range, we could argue that as a very basic requirement, the metric would be on an ordinal scale, for example:

$$p(stay\_home) \leq p(go\_shopping) \leq p(use\_credit\_card) \leq p(mortgage\_application)$$

This would be a minimum requirement for this hypothetical metric to be meaningful—or fulfill the representation condition as expressed in the area of measurement theory (Fenton & Pfleeger, 1998). It should be obvious that the exact initial level as well as change of privacy cannot be established. This is not only because privacy is qualitative and perhaps subjective, but also because we have no control or knowledge of all variables affecting it. For example, how many monitoring technologies (such as CCTV elements) have invaded our private space, and to whom is the captured data available? For how long? What is the quality of the captured data and therefore the likelihood of positive identification? What protection does the legal system provide against third-party enquiries to access the data? It can be seen that not only the number and diversity of these questions can be exceedingly high, but also answering them is challenging in principle.

Determining qualitative variables in uncertain and open problem domains has been a major topic of interest in the discipline of macroeconomics. The well-known so-called cross methodology has significantly contributed to the understanding of the market forces of supply and demand (Dornbush & Fischer, 1998; Branson & Litvack, 1981). The remainder of this section deals with porting these proven techniques to the domain of privacy and security.

Initially we need to classify the relevant technologies in two "markets": the security technologies and the adversarial technologies. By security technologies we mean those that intend to support the confidentiality of our private data, such as firewalls, antivirus tools, and so on. In other words, these are defensive technologies and primarily access control measures. By adversarial technologies we mean those technologies that are used for testing our security technologies. These are hacking tools, such as vulnerability scanners, exploits, security assessment frameworks. These offensive security mechanisms are required in order to be able to assess the security level of an IT infrastructure. A key differentiator is the purpose or intention of use of a certain technology. In the security technologies market, the technologies can only be used for benign purposes, whereas in the adversarial technologies market, the technologies can be used for either benign or malicious purposes. "Ethical hacking" for instance is the term used for capturing the benign use of the adversarial tools.