1-28-2009

The Intersection of Privacy and Security

Sue Conger
University of Dallas, sconger@gsm.udallas.edu

Brett J. L. Landry
University of Dallas, blandry@gsm.udallas.edu

芽|Sprouts Working Papers on Information Systems ISSN 1535-6078

The Intersection of Privacy and Security

Sue Conger
University of Dallas, USA

Brett J. L. Landry
University of Dallas, USA

Abstract
There is a common misconception that privacy and security are the same thing. The reality is that while there is an intersection of these two topics, there are differences between security and privacy. This paper sets up through illustrations some similarities and differences between these topics.

Keywords: Privacy, Security, Confidentiality, Integrity, Availability, Non-repudiation, Fair Information Practice, Anonymity, Fair use, Access, Life cycle, Integration

Permanent URL: http://sprouts.aisnet.org/8-38

Reference: Conger, S., Landry, B.J. L. (2008). "The Intersection of Privacy and Security," University of Dallas, USA . *Sprouts: Working Papers on Information Systems*, 8(38). http://sprouts.aisnet.org/8-38

The Intersection of Privacy and Security

Abstract

There is a common misconception that privacy and security are the same thing. The reality is that while there is an intersection of these two topics, there are differences between security and privacy. This paper illustrates similarities and differences between these topics.

Background

The purpose of this paper is to begin to develop understanding of the differences between privacy and security. This differentiation is important because many practitioners and researchers discount the differences and assume that by providing a secure computing environment that privacy is also served. We offer anecdotal evidence that this notion is untrue and develop new areas for privacy and security researchers to further explore the differences. The arguments presented here also raise empirical and contingent questions about the frequency, generalizability, and importance of the differences identified.

Many analogies can be drawn from different areas of life experience. For example, consider the idea of stuffing money under the mattress. People who are often distrustful of banks or have income that they want to keep unrecorded will often stash cash at home. This cash is private because banks and the IRS do not know about it. Thus, hidden cash is a form of private wealth. But, is the money secure? No; for money to be secure, it should be insured and stored in an institution that can offer some level of guaranty, such as a bank. The same relationship holds true for many situations relating to Information Technology (IT) privacy and security.

Consider the example of Internet email. By default, Internet email is neither private nor secure. Basic security and privacy can be added by simply employing passwords on computers and accounts. Further privacy is added via encryption so that the message cannot be altered or read by unauthorized personnel. At this point the message is private given that the encryption employed and the keys are sufficient and, because of passwords, there is some security. However, information transmitted via email may breach corporate security or leak customers' Personally Identifiable Information (PII). Therefore, even with privacy, security can be breached. To summarize this relationship, privacy does not offer security; there cannot be privacy without also having some security.

The next sections of the paper define privacy and security constructs and characteristics that are the basis for this research. Then, the commonalities between privacy and security are developed. Next, intersections of privacy and security are discussed to develop understanding of the differences of the constructs. From the intersection, directions for research to further develop our understanding of the differences between privacy and security are discussed.

What is Privacy?

Privacy has many facets and can be defined in many ways. Personal privacy generally applies to keeping confidential anything an individual does not want known, such as a person's location

(Solove, 2006). For our purposes, privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967). Westin's definition is appropriate by its applicability to both individuals and institutions, and its focus on information. Therefore, in this research, this definition describes *information privacy*.

Characteristics of privacy include anonymity, fair use, and controlled access, life cycle, and use for integration (Culnan, 1995; Clarke, 1999; Gellman, 1998; Solove, 2004). No empirical research validating these characteristics could be found, thus, each is debatable and a subject for further research. Each of these characteristics is defined in this section.

Anonymity is defined as "of unknown authorship or agency" and "bearing no name" (Landau, 1992, p. 29) and usually applies to written materials. In this research we adapt this definition to relate to personally identifiable information (PII) for customers, employees, clients, volunteers, etc. about whom information is collected by organizations. While a whole suite of Privacy Enhancing Technology (PET) has developed in the last ten years, most organizations do not use it. Nor do organizations routinely encrypt data as a gross method of protecting records. Evidence of this problem is reported almost daily by Attrition.org's breach list which shows a doubling of data leaks around the globe (Attrition.org, 2008). Thus, anonymity is problematic in many organizations.

Fair Use concepts stem from two sources – OECD Privacy Guidelines (1980, 1998) and U.S. Fair Information Practices (Culnan, 1995; U.S. Privacy Act of 1974). In essence, the principles address limited data collection relevant to the context, limited data usage disclosed before use, protection against unauthorized access or use, no sharing, and all with that data subject's consent.

Access is defined as "right to approach, use, etc." (Landau, 1992, p. 5). "Privacy depends on degrees of accessibility of information..." (Solove, 2004, p. 213). Access is partially covered under Fair Use concepts but those concepts assume no movement off organizational premises by authorized persons, and, therefore, do not go far enough to cover requirements for, e.g., encryption, or restricted location/device characteristics that today's uses require. Therefore, this extended view of access is developed as a separate concept.

Use usually refers to using data for other than agreed upon uses by the collecting organization. In this research, 'use for integration' refers to the industry practice of 3rd parties taking data from disparate sources for purposes of integration, profiling, and resale (Solove, 2004). This use of PII had not developed when the U.S. Fair Information Practice and EU Fair Use practices laws were developed. Therefore, integration (as a negative characteristic of privacy) is developed as a separate concept.

What is Security?

Security is the condition of being protected against danger or loss Security typically is associated with characteristics of Confidentiality, Integrity, and Availability (CIA), all of which are controlled to implement computer security. A fourth characteristic, non-repudiation is

increasingly viewed as a requirement of secure computing. Each of the characteristics is defined in this section.

Confidentiality is defined as "assurance that information is not disclosed to unauthorized individuals, processes, or devices" (Krutz and Vines, 2004). It is important to note that confidentiality is different than privacy. Access is granted or denied based upon authorization and therefore information can be confidential but not private.

Integrity is accuracy of the information and the IT controls in place to protect against unauthorized modification or destruction. It is possible for information to be private but not have integrity because it can be modified or deleted (Merkow & Breithaupt, 2005).

Availability is timely, reliable access to data and information services that are restricted for only authorized users (Krutz and Vines, 2004; Merkow & Breithaupt, 2005) Among the CIA components, Availability is probably the most antithetical to privacy in that making information available makes it public that is, not private.

Finally, Non-Repudiation is the assurance that a sender of "data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data" (Krutz & Vines, 2004). As we examine the differences between Privacy and Security, we will see that in all cases non-repudiation has a negative relationship to privacy characteristics.

Commonalities between Privacy and Security

There are areas of commonality that are also a source of some of the conceptual blurring of boundaries between privacy and security. Some organizational commonalities might include corporate policy, governance, training, and technical implementation.

The purpose of corporate policy for both privacy and security is to identify the position of management relative to the topic, delegate responsibility, identify the scope of policy affect, define compliance requirements, and define reprisals for lack of compliance. Corporate policy drives actions and cultural response to privacy and security needs. Privacy and security are treated as one in many companies and only with the huge number of data leaks and breaches are coming to be understood as different.

In many companies, the corporate and technical groups responsible for security (which has had corporate awareness of need for over 20 years) are also responsible for privacy. Training of staff can cover both privacy and security in single session. Corporate statements of privacy and/or security for which many companies require annual reading and signing, can also incorporate both concepts in one page. In implementation, sometimes privacy and security are served by the same actions. The many commonalities have contributed to the conceptual confusion between privacy and security. Additionally, the technical implementation of security and privacy programs can use the same hardware, software, often are maintained by the same technicians.

Clearly, there are commonalities of privacy and security. In large data breaches, both privacy and security can be lost. The 2007 data breach at the U. S. Department of Transportation (DOT) is just one example of this common aspect of privacy and Security. In the DOT example, the daughter of a teleworker installed Limewire P2P Sharing software on her mother's computer, inadvertently sharing DOT and National Archives files across the Internet (Broach, 2007). While this is a clear example of both security and privacy being lost, there are other examples where the intersections differ depending on the components of privacy and security examined.

Intersections of Privacy and Security

Evaluation of the intersection of privacy and security allows us to tease out implementation considerations in different situations. There are many ways to look at the privacy-security intersection; this paper concentrates on the intersection of data and agent actions as they each relate to privacy and security characteristics. Privacy considerations include anonymity, controlled life cycle, monitored use, fair use (CITE), controlled access, and the negative notion of data profiling and integration. Security considerations include CIA – confidentiality, integrity, and availability as well as non-repudiation.

The intersections of data and agents are evaluated through a series of tables looking at the privacy and security concepts in light of data privacy - agent security, agent privacy - data security, data privacy - data security, and agent privacy - agent security relationships. Data are typically thought of as the focus of privacy and security. Data refers to information used in an application and may relate to, for instance, manufacturing transactions, employees, application users, customers, and so on. Some data are subject to privacy requirements more than other data. Regulatory laws may dictate privacy and/or security functional requirements. HIPAA, for instance, is an example that requires patient data to be kept secure (security requirement) and have restricted access (privacy requirement), thus mixing the concepts of privacy and security in a single set of requirements (HIPAA, XXXX).

Agents are the actors who might access, change, or copy data. Agents include not only authorized application users, security staff, database staff, and computer operations staff, but also include unauthorized employees, hackers, or other who seek access but are not authorized.

Each of the four figures presents a discrete view of privacy and security constructs in a different context of analysis. The only construct that shows a consistent relationship across the four types of analysis is non-repudiation. That is the data privacy - data security, data privacy - agent security, agent privacy - data security, and agent privacy - agent security privacy -- non-repudiation relationships are consistent for all privacy constructs.

Anonymity and integration/data profiling demonstrate a negative relationship with non-repudiation. Recall that non-repudiation is the ability to identify with certainty either an agent or some data. It is reasonable that this certain identification is antithetical to anonymity. Further, by integrating data in some way, non-repudiation becomes impossible, therefore it also demonstrates a negative relationship.

The privacy characteristics of controlled life cycle, monitored use, Fair Use, and controlled access all exhibit a positive relationship to non-repudiation. This means that with controlled access, for instance, non-repudiation should also be possible, and vice versa.

To demonstrate the reasoning that underlies the designation of each cell, anonymity and its relationships are traced through all four figures. Anonymity is chosen because, like availability, it exhibits all relationships – supporting, negative, and neutral, depending on the data-agent relationships involved.

Data privacy - data security and agent privacy - agent security anonymity and confidentiality support each other. By support, we mean data (agent) anonymity supports or positively relates to data (agent) confidentiality. Confidentiality relates to the maintenance of a secure environment against leakages while anonymity relates to the lack of individual record (or person) identification. Thus, while similar, the concepts are different. In the data privacy - data security and agent privacy - agent security dyads, the relationship is a supporting one such that by the presence of one condition, the other condition is facilitated.

Data / Data		**Data Privacy**					
Data Security		Anonymity	Controlled life cycle	Monitored Use	Fair Use	Controlled Access	Integration & Data Profiling
	Confidentiality	Support	Support	Support	Support	Support	Negative
	Integrity	Neutral	Neutral	Support	Support	Support	Negative
	Availability	Neutral	Negative	Negative	Negative	Negative	Support
	Non Repudiation	Negative	Support	Support	Support	Support	Negative

Figure 1. Data Privacy and Data Security Intersection

Agent / Agent		**Agent Privacy**					
Agent Security		Anonymity	Controlled life cycle	Monitored Use	Fair Use	Controlled Access	Integration & Data Profiling
	Confidentiality	Support	Support	Negative	Support	Negative	N/A
	Integrity	Neutral	Support	Support	Support	Support	Neutral
	Availability	N/A	Support	Support	Negative	Negative	N/A
	Non Repudiation	Negative	Support	Support	Support	Support	Negative

Figure 2. Agent Privacy and Agent Security Intersection

In the data privacy - agent security condition (Figure 3), data anonymity and agent confidentiality exhibit a neutral relationship. By neutral, we mean that regardless of one state (e.g., data anonymity), no inferences about the state of the other characteristic (agent confidentiality) can be made. For example, data on Wikipedia, whether valid or not, is

anonymous. Since the data is anonymous, agent confidentiality can be maintained or not as desired.

Conversely, in Figure 4, agent anonymity is counter or negatively related to data confidentiality because with agent anonymity one would expect breaches to increase. Therefore, a condition of security would be no agent anonymity.

Agent / Data		**Data Privacy**					
Agent Security		Anonymity	Controlled life cycle	Monitored Use	Fair Use	Controlled Access	Integration & Data Profiling
	Confidentiality	Neutral	Neutral	Negative	Neutral	Negative	Neutral
	Integrity	Context	Support	Support	Support	Support	Negative
	Availability	Neutral	Neutral	Neutral	Neutral	Neutral	Neutral
	Non Repudiation	Negative	Support	Support	Support	Support	Negative

Figure 3. Data Privacy and Agent Security Intersection

Data / Agent		**Agent Privacy**					
Data Security		Anonymity	Controlled life cycle	Monitored Use	Fair Use	Controlled Access	Integration & Data Profiling
	Confidentiality	Negative	Support	Support	Support	Support	N/A
	Integrity	Negative	Support	Support	Support	Support	Negative
	Availability	Neutral	Neutral	Support	Support	Support	Support
	Non Repudiation	Negative	Neutral	Support	Support	Support	Negative

Figure 4. Agent Privacy and Data Security Intersection

One cell in Figure 3, relating to data anonymity and agent integrity, can exhibit either a supporting or negative relationship depending on the context. For instance, in a company setting, data anonymity is likely to exhibit a supporting relationship to agent integrity as an individual is unlikely to change data that is not known to them. That is, a student might want to change a course grade but, with student anonymity, the transgressor won't know which grade to change. In contrast, in a setting such as Wikipedia, data anonymity may negatively relate to agent integrity. The agent is more likely to change data in a self-serving way *because* the data is anonymous.

Discussion

This paper seeks to raise issues and heighten awareness of privacy and security as separate constructs, consisting of distinct characteristics. We hope to raise debate and discussion on the

issues presented. We do not feel completely comfortable that our assessments might not be changed through empirical research; in fact, we believe that each cell of each figure should become an area for further research consideration to tease out the nuances and variations of the relationships discussed.

The concept of 'Target of Evaluation' (TOE) is one that focuses attention on different facets of a context, such as data privacy, agent privacy, contextual privacy, and so on. These different facets have the potential to alter the outcome of the analysis by changing the privacy/security characteristic relationships. Further, data is not a monolithic entity since the issues vary for data 'at rest,' 'in transit,' and being accessed. The 2008 Hannaford data breach in which hackers installed malware on internal servers to capture credit card data in transit (Messmer, 2008). Thus, even by following all Payment Card Industry (PCI) security regulations, privacy breaches are not protected against. . Thus, other targets of data evaluation are needed to present a complete view of data privacy/security issues. Just because industry security guidelines are met does not mean that privacy concerns also are met. A similar situation seems to exist for agent access. Agent restrictions in applications can be either functional, data-related, or both. These multiple ways of thinking of agent capabilities should also be subjected as targets of evaluation.

Conclusion

While security addresses some privacy characteristics, and privacy implies some security characteristics, the two constructs are distinct and should be treated separately. Which is a greater concern -- to have security or privacy? As this discussion attests, this is no simply question and the question has no simple solutions. The intersections between privacy and security demonstrate that the trade-offs needed require consideration of many varied situations and that the situational context itself may change the relative relationships between the privacy and security characteristics. As a result, developing only a secure view of a computing environment all but guarantees that privacy issues will be unsupported and, therefore, problematic.

References

Broach, Anne, "US Congress: P2P Networks Harm national Security," 2007. cnet.com

Clarke, Roger, "Internet Privacy Concerns Confirm the Case for Intervention," *Communications of the ACM*, Feb 1999 42(2), pp 63-67.

Culnan, Mary, "Fair game or Fair Play?" *The Journal of Business Strategy*, Nov/Dec, 1995, 16(6) pp. 29-31.

Gellman, Robert, "Does Privacy Law Work?" in *Technology and Privacy: The New Landscape*, (Philip E. Agre and Marc Rotenberg, Editors), Cambridge, MA: MIT Press, 1998, pp.193-218.

Kurtz, Ronald &Russell Vines, *The CISSP Prep Guide*, Second Edition, NY: John Wiley, 2004..

Landau, Sidney, Ed., *Webster's Illustrated Contemporary Dictionary*, Chicago, IL: Ferguson Publishing, 1992.

Merkow, Mark & Jim Breithaupt, *Computing Security Assurance: Using The Common Criteria*, NY: Thomson, 2005.

Messmer, E. (2008) Details emerging on Hannaford data breach retrieved from http://www.networkworld.com/news/2008/032808-hannaford.html

Solove, Daniel J., *The Digital Person*, NY: New York University Press, 2004.

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

Office:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org

芽|Sprouts