Personal Information Privacy: The World Has Changed

Sue Conger, University of Dallas, Irving, TX 75062, USA; E-mail: sconger@aol.com

ABSTRACT

Individuals can no longer manage their own personal information privacy. Rather, corporations and organizational entities with which individuals interact must recognize vulnerabilities and actively manage their data to guarantee known data sharing and to prevent data leakages. A more complete model of consumers' personal information privacy that includes not only data gathering, but also data sharing and data leakage is presented and defended here.

1. INTRODUCTION

Daily, we read of some new data loss of millions of individuals' personal information [1, 17, 32]. As losses amass, the realization that personal information privacy (PIP) is no longer manageable by individuals becomes clearer. Yet, research to date proposes that PIP is the responsibility of individuals' forging contracts with corporations for protection of their data [28], that it is the responsibility of government to protect the individual [29], or the responsibility of corporations to manage internal use [27, 28]. These views are all corporate-centric but threats have expanded beyond the corporation to its data-sharing partners. This shortcoming appears due, in part, to an incomplete view of corporate vulnerabilities. In this research, we build on past privacy research to develop a model of data sharing from the individual to the corporation and from the corporation to its data-sharing partners.

The premise of this research is that the individual-to-corporation link, while still needing research, is well understood. However, what businesses *do* with the data, once collected, is less understood and is becoming more important to privacy maintenance [cf. 1, 32]. Corporations, having spent billions creating secure corporate silos, do not operate in a silo-like vacuum. Rather, corporations routinely share data with business partners and legal entities that in turn, share that data with other organizations. In this data-sharing environment, we develop three types of data sharing *partners* with which corporations interact and the need to actively manage or prevent different types of data access and use. Once the full extent of data movement is understood, it is clear that corporate policies and procedures need extension and regulation to control multi-party access. In the next sections personal information privacy (PIP) research to date is summarized, the expanded model and data supporting it are presented, and suggestions for further research are developed.

2. PERSONAL INFORMATION PRIVACY MODELS

Two distinct periods of PIP research are summarized. Pre-Web maturity research concentrated on organizational data gathering, usage, and access practices, seeking to articulate the issues relating to PIP and organizational data gathering and use. Post--Web maturity research shifted focus to Internet transactions that generate more and different data, use more and different methods of data collection, and have different persistence issues. Through these discussions we argue that the World Wide Web (Web), a new technology 13 short years ago, changed many of the issues relating to PIP and furthermore, the Web and emerging technologies enable new abuses of data that require corporate relationship and data management.

2.1 Personal Privacy Before Web Maturity

Research published before Web capabilities matured had few references to Web information gathering practices [cf. 10, 28]. Much research in the 1990s sought to determine the scope of the privacy problem and how to frame privacy issues [8; 11, 18, 28,]. Privacy, at a minimum, concerns collection, unauthorized secondary use, ownership, accuracy, and access [18, 28].

Culnan & Armstrong's [10] privacy leverage model relates corporate use of consumers' collected personal data to the trust that either leads to retention or defection of customers. Culnan's model demonstrates an understanding of the issues in organizational data collection and use but assumes solid control over all use and also assumes firm's have some policy (whether explicit or not) on PIP protection. Transaction decisions are based on a 'privacy calculus' that is an idiosyncratic trade-off between trust, risk, cost/benefit, and other consumer assessments [2, 3, 10; 14, 20, 24, 25]. Further, this research assumed that 'demographic' and transaction data were the types of data gathered; this is no longer the case.

2.2 Personal Privacy After Web Maturity

Research published after 1998 (when Web transaction technology matured) demonstrates that the Web enables novel methods of obtaining information on individuals, some of which is unrelated to transactions between consumers and corporations. Web privacy issues include where and how information is collected, whether or not the collection is known or unknown by the consumer, trust in the vendor (see Figure 1) [15, 20], the life and breadth of information collected [13], perceived benefits and risks of information sharing [12], methods of storing and using the information and corporate privacy policies [13]. Web purchase transactions research includes consumer, product, medium, merchant, and environment characteristics [2, 3, 5, 6, 13, 14, 15, 19, 20].

The research summarized in Figure 1 addresses part of the transaction chain and tends to omit feedback from a transaction as paramount to future transactions though some research includes feedback [cf. 3, 10]. Omitting feedback implies similarity of evaluation for any transaction with a company whereas evidence supports the notion that every transaction is affected by all past transactions and transactions with other companies as well [21, 22]. There is conceptual confusion on whether the individual's assessment of a potential transaction results in perceived risk or perceived trust, or both [6, 13, 14, 15, 19, 20]. Most research never states what data is collected, or describes a limited domain of data that oversimplifies breadth of data that might be collected [cf. 13, 14, 20].

3. AN EXPANDED MODEL OF INFORMATION PRIVACY

This section builds on past privacy research to present a more complete view of the current state of PIP. The expanded model of information privacy has as its basis, the past research on how an individual, the 1st party, comes to transact with a company, the 2nd party vendor/provider (5, 10). Each unshaded box in Figure 2 and the arrows depicting the relationships between them represent areas in which significant research has already been conducted and incorporates the bodies of work summarized in (10) and (5). Part of the individual's decision includes what data to provide to the 2nd party based on the expected life and use of that data, perceived reasonableness of the data collected, expected benefits, and expectations of corporate use of the collected data (9). These new concepts are in Figure 2. The shaded boxes and arrows depicting their interrelationships represent areas in which little or no research has been published.

The type of data requested leads the consumer to draw conclusions about the perceived reasonableness of data being collected. Perceived reasonableness of data is a new construct in the decision calculus that arises from corporate use of smart technologies that can surreptitiously collect such data as click streams, personal movements, food and medicine usage, genetic markers, DNA, health, or other biological data, and criminal, genealogical, or financial history [9]. The decision calculus results in an assessment of trust and risk, to either consummate or cancel the transaction and, if consummated, which data to share and the sharing duration.

Figure 1. Summary model of Web transaction issues (Adapted from 5)

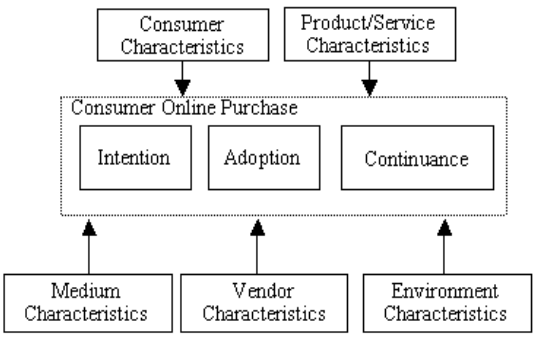
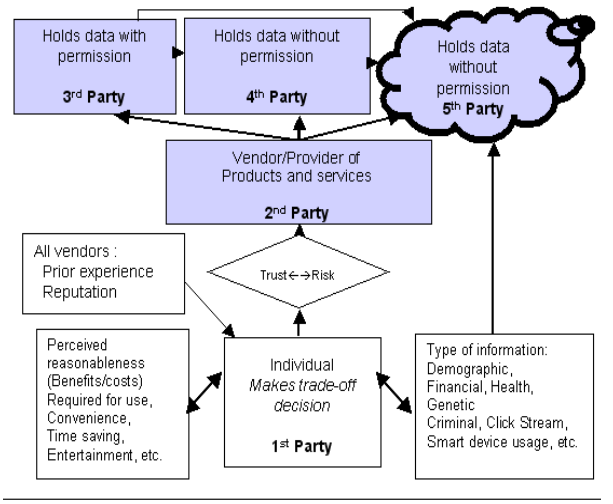


Figure 2. Expanded privacy model (Adapted from 9)



Data may be collected before; during, or after an actual business transaction and the data collection may be known or unknown by the consumer. Combined with other transactional and post-transactional data, this data enables the building of a consumption profile for a family that could affect their insurance or medical coverage. Combined with the other purchase information, a decision profile for the household might be developed and used for discrimination [9].

Consumers appear ignorant of corporate privacy policies and rely heavily on organizations that vouch for the trustworthiness of the vendor (20). The proposed model incorporates real policies and procedures (P&P), perceptions of those P&P, and indications of trustworthiness on Web or other sites.

After a transaction is complete, the information is shared with any number of legal data-sharing entities, the 3rd-party data user who is a known external data-sharing partner, for example, a credit reporting company such as Experion who shares data with 2nd-party permission. Companies, such as Experion, generate their revenues by matching consumer information to transaction information, profiling consumers, and reselling the expanded information. The Experions of the world are not necessarily the problem unless their use or access to data violates their legal and contractual agreements. The greater vulnerabilities arise from Experion's data sharing partners, the 4th parties.

Third-party organizations resell or provide their information to 4th-party organizations through legal requests. Problems arise when 4th-party partners use data without 1st-party and/or 2nd-party permission. Such partnerships might be governmental pre-emption of data (8) or legitimate data-sharing partners of the 3rd-party who violate the terms of their agreements. There is no actual way for, for instance Experion, to ensure proper use since compliance is self-reported. Further, government cooption of data has come under increasing scrutiny as violating constitutional rights to privacy provisions (32).

The nebulous cloud with fuzzy boundaries identifies the last category: 5th-party data users. This category of 5th-party users, are unintended, unwanted, and often unethical and/or illegal users of vendor data. Fifth-party usage results from non-compliant employee behaviors that result in leakages or from illegal activities. Fifth-party data users obtain data without permission or knowledge of their sources, which may be 1st, 2nd, 3rd or 4th parties (4, 17, 32). People who steal computers and who leak names, addresses, and, e.g., financial information, are in this category (32).

From ChoicePoint's infamous identity theft in February, 2005 through 2006, there have been 438 thefts, hacks, or leakages of consumer information of which 335 organizations reported losses over 181 million individual accounts with social security information (33). The 103 organizations either not reporting or not including SSNs, would approximately double the number of transgressions (33).

4. DISCUSSION AND FUTURE RESEARCH

Leakages of data by corporations and governments, while serious, are only evidence of inadequate or unmanaged policies and procedures. This section discusses research needs to determine both a more accurate scope of these problems and how to obtain equitable, workable solutions.

As much as the individual decision process has been researched, there is no known research on parties three through five, nor is there research on the impacts of data leakages or data sharing, in general. While there is a growing body of research on privacy policies and procedures [e.g., 22, 26], no evaluations to date include the impact on consumer decisions. Sample hypotheses for evaluating companies' data sharing management practices might include the following:

- The extent to which the individual's experience with this company's and other companies' data leakages affects the current decision.
- The impact of vendor policy and procedure management for internal users on actual data access and use, and the related impacts on consumer decisions.
- The impact of vendor policy and procedure management for data sharing with known 3rd-party and 4th-party companies on the consumer's beliefs about the company trustworthiness, and related impacts on consumer decisions.
- The impact of vendor policy and procedure management for preventing data leakages to 5th -party users on consumer beliefs about the company trustworthiness, and related impacts on consumer decisions.

The expanded model of personal information privacy described should become the basis for future PIP research.

5. SUMMARY

The expanded model of personal information privacy builds on past research to address emergent issues relating to heretofore unprecedented information demands of governments, unacknowledged corporate information sharing, and the spate of leakages of information from business organizations. The model describe five type of information users from the original owner to the vendor with which they conduct business transaction, to the data vendor, to legal fourth parties, to illegal fifth parties. Individuals are incapable of managing five sets of relationships. Rather, each vendor collecting any customer information must become responsible for actively managing the same criteria with its data-sharing partners *and* their data-sharing partners. Further, all organizations need to improve their management of data leakages to stem the deluge of data losses.

6. REFERENCES

Available on Request