Vampire Bats: Trust in Privacy

Tracy Ann Kosa
Faculty of Science
University of Ontario Institute of Technology
Oshawa, Ontario
tracyann.kosa@uoit.ca

Abstract—Trust and privacy are ancient social concepts. Work on formalizing trust dates back to the mid-nineties, while work on formalizing privacy is in its infancy. The two concepts have a number of similarities including considerations of information type and sensitivity to inform actions, relationship between the communicating parties, and the context or purpose for communication. There are some key differences. Privacy, unlike trust, is legislated. In Canada, there are also a number of regulations, directives and policies that come along with the legislation. Trust, on the other hand, is the Wild West; almost anything goes. Early attempts at formalizing privacy have been largely restricted to P3P initiatives and other policy developments. Not only have they been largely ignored by the user community, but also because of the limited scope in application seem to fail to actually enable privacy protection. On the other hand, early trust models have taken a different approach. Instead, using a natural science approach and artificial agents, trust is circumscribed, simple and most importantly - repeatable. In the context of failed attempts at formalizing privacy through policy, learnings from trust can be utilized to advance the computational notion of privacy protection. This paper takes the work on formalizing privacy in a much needed new direction by examining the potential of an appropriate and applicable framework for privacy based on extant trust formalizations. It proposes a formalization for privacy can be based on trust, and would outline the types of privacy, examine privacy based decision-making, and explore the applicability of the agents as appropriate representations of people in the computational environment.

Keywords-privacy, trust

I. INTRODUCTION

Social conceptions of trust vary greatly, but are very commonly related to a belief in good character. They can also be related to actions that two parties are taking together; e.g. trusting the driver of the car when you’re the passenger. At its essence, trust is a measurement of what is otherwise unknown because it cannot be verified.

Trust can be examined as a continuous measure, as in evaluation or reliability assessments, or a binary decision point when referring to a decision. As a subject of ongoing research, it also involves related concepts such as confidence. Coleman offers a few key points about trust as an action:

1. Where there is incomplete information, trust allows for people to take an action, e.g. get up in the morning (Luhmann);
2. The relationship between the trustee and the trustor depends on trustworthiness of the trustor, where trust is a voluntary action with no guarantee;{Similar to the prisoner’s dilemma.}
3. Time passes between the decision to trust and the result of a trust action. (Coleman, 1998)

These characteristics focus on trust behavior, which assists in the application of trust to computer science (CS) and the consideration of risk, reliability and reputation as related to trust. Power is a concept related to trust. For details see Fukuyama and Yamagishi and the related discussions on security and trust.

While social scientists have worked within the fluidity of this realm for years, CS requires the language of trust to be normalized. In this sense, interpersonal trust is more about the acceptance of risk to support action, where computational trust tends to be about transactional reliability and authenticity. These concepts are related, but can be examined separately.

Similarly, privacy is historically treated as an emotional and ethical concept. Social conceptions vary greatly, and there is much anecdotal evidence on people’s feelings about privacy, violations of privacy and the distinction between public and private space. In fact, the idea of informational self-determination is one that legal scholars and privacy advocates discuss at length. In the North American context, legal recognition of informational privacy as a distinct civil harm is usually traced back to the right “to be left alone”. (Warren and Brandeis, 1890) In the later part of the 20th century, states began to regulate increasingly aggregated collections of personal information in the public and private sector through
data protection legislation. (Clarke, 1999) Legislation first came to Canada in the form of the Personal Information Protection of Electronic Documents Act (PIPEDA). It is worth noting that data protection laws are, at best, mechanisms for promoting privacy. (Brown, 2009) They tend to shift the focus from the ability of the individual to control their information to the appropriate management and handling of data by organizations. As in trust, there is a distinct and critical difference between an individual’s privacy and an organization’s data protection practices.

Assuming formalization is a good thing, and striving to place trust and privacy in the computational context, this paper first examines the concepts of trust and privacy respectively, moving on to a discussion of the similarities and differences in Section 2.1 and 2.2 respectively. Section 3 provides an overview of the existing attempts at formalizing privacy. Section 4 provides an overview of the first trust model, and an analysis of why it might work for privacy in Section 4.1. Conclusions are presented in Section 5.

II. TRUST AND PRIVACY

Although historically socially analyzed, both trust and privacy can be examined using a natural science approach. The foundation of the applied sciences, the natural science approach allows for repeatability in the use of the trust and proposed privacy models.

A. Similarities

Trust and privacy are both common phenomena. While trust may be more required for human function and privacy more for human interaction, they are both necessary for day-to-day life. In order to be enabled at the technical level, both need to be formalized. Agents, autonomous pieces of code that are pseudo-intelligent, can represent trust in a computational environment. (Marsh, 1994)

Trust and privacy are both essentially intangible human values. They are highly information type and sensitivity specific; relationship-dependent and purpose driven. The trust I may place in my sibling to drive me to the airport is significantly different from that which I place in him to fly the plane I will ride in. The privacy I place in my priest is different than that of the arresting police officer. Likewise, I may trust my doctor with the privacy of my AIDS test results, but not my jilted lover. In order to compute such value laden terms, both trust and privacy require agreed upon semantics.

Trust itself is operational risk; all trust involves some element of risk. (Luhmann, 1979) Privacy is also always a risk-based decision; particularly when it comes to information disclosure.

This paper supports the idea that trust and privacy are both continuous measurements, not on and off switches. The level of trust, as with the feeling of privacy I may have, with a given person change based on the next experience, an additional piece of information, or a change in environment. I may comfortably discuss my fears with my therapist in her office, but not on the subway platform.

Trust, like in privacy, is also impacted by groups; although how and why helps demonstrate some of the differences between the two concepts.

B. Differences

Where trust has a positive correlation to privacy, privacy is negatively related to trust. Perceptions of trustworthiness may increase the tendency of people to share information willingly, thus giving up their privacy for a benefit (real or perceived). Yet, the exercise of privacy may impede trust; if I choose to withhold information, about for example, my identity the second party is less likely to trust me in the given exchange.

Fukuyama and Yamagishi both discuss how collectivist societies increase security so significantly that trust either isn’t necessary (Fukuyama) or never develops at all (Yamagishi). Traditional social science research on privacy demonstrates that the opposite; closed groups can lend themselves to more privacy.7

Where privacy is legislated, trust is not. There are pros and cons to the use of legislation, the discussion of which is beyond the scope of this paper. However, the existence of legislation changes the nature of the approach to privacy in ways that are not applicable to trust. For example, legislation typically results in a number of administrative and auditing related processes that any proposed privacy model would have to consider in order to be practical. 8

Concepts of trust do, however, pop up in the health, private and public sector privacy legislation, although the use of the terminology is often confused. In health, the term “custodians” is used to reference trusted third parties and / or health care providers. For example, “trustees” of personal health information is a term used in Ontario’s Personal Health Information Protection Act (PHIPA) to reference persons who make health care related decisions on behalf of those who cannot decide for themselves.

The implementation of public sector privacy legislation rests of a delegation of authority, a document used to transfer responsibility for administration of the privacy law from the Minister to a civil servant. That civil servant is considered the ‘authority’ for privacy issues, and is trusted to act on behalf of the Minister in making decision on privacy on a day-to-day basis – hopefully in consultation with program areas

---

7 E.g. social networking sites like Facebook, and the illusion of ‘privacy’ within the circle of friendship despite being online. See Dwyer for additional details.

8 This does not explicitly consider the fact that the assumed objective of privacy legislation is to protect privacy. In practicality, it seems more likely that the objective of these laws is to regulate organizational information management practices and limit liability in respect of data protection.
throughout the ministry.

In addition, the public sector legislation substitutes the traditional consent requirements with a combination of statutory authority (e.g. a law must be passed to enable a ministry to collect personal information) and a notice of collection (a publicly available document that informs people what the Government does with their information).

In the private sector, the Personal Information Protection and Electronic Documents Act (PIPEDA), requires organizations to actively obtain consent from people in managing their information; effectively setting out a lower threshold for trusted actions with personal information by companies than by Government.

III. FAILED PRIVACY MODELS

Within computer science (CS) there have been some attempts at developing a computational privacy framework; the majority of this work can be divided in to two groups: policy-based work and theoretical ontological frameworks.

A. Ontologies

Ontological research takes a more traditional CS approach to privacy. There are three different approaches to privacy ontology: policy enforcement based (Hassan and Logrippo’s ontology for privacy policy enforcement), industry specific (Hecker’s privacy ontology to support e-commerce), and general to the legislation (Teng’s privacy ontology for interpreting case law). There are some similarities in the privacy ontology research. Each of the ontologies specifies some method of formalized representation of legal requirements, which is significant difference in privacy – the only legislated area of CS. They all follow the same steps, outlined by Hecker et al, in the creation of the privacy ontology, (1) define a glossary of terms, (2) define static model concepts, including resources, entities and relationships, (3) identify safeguards to protect resources, and (4) identify the processes that apply.

The privacy policy enforcement ontology is built on much of the policy-based research in CS, so its applicability varies; e.g. the ontology proposed by Hassan and Logrippo is based on a set of privacy principles specific to Canada so it could only be applied in this jurisdiction. This ontology is limited because of the jurisdictional construct; while data flows are not restricted by geography.

Hassan and Logrippo note that “our approach is far from covering all aspects of privacy law, in fact we are not even trying to approach such completeness, since ethical, social and other aspects can be impossible to represent in logic-based semantics.” (Hassan, undated) Yet, their proposal purports to accomplish just that in order to calculate privacy policy enforcement.

Hecker et al’s work includes a similar process ontology which can identify the resources and data subject. However, the authors note that the very purpose of Web 2.0 – information dissemination – is the anti-thesis of privacy. They go on to explore the concept of how generic privacy ontology can be used to remake the architecture of e-commerce transactions to be privacy friendly and encourage capitalism, but do not address the core questions around the possibility of re-architecting the Internet as we know it, so that Web-based transactions simply did not require the transfer of personal information at all.

Tang and Meersman set out to apply ontological technology directly to regulated privacy requirements, by linking case law and legislation. In this environment, the proposed ontology would be represented by fact lexons (extracted from case law) and the directive commitments (that tailor fact lexons to ascribing real life application requirements). Tang and Meersman are some of a very few researchers in ontological field of privacy that propose a development environment: DOGMA (Developing Ontology-Guided Mediation for Agents), as it separates concepts and relations from constraints, derivation rules and procedures. (Tang, 2005) However, no testing has been done to date on the application of such a model.

B. Policy

This research generally falls within policy creation, breaches and assessments. Popp and Poindexter focus on the creation of policies, arguing for the coordination of security and privacy policies. While this approach is common within the CS domain, it fails to recognize the instances where security and privacy do not converge, and may in fact conflict. While the authors highlight the typical privacy protections: privacy appliances, data transformations, anonymization, selective revelation, immutable audit and self-reporting data, they fail to demonstrate an understanding (as Hecker et al, 2008) that a key privacy protection is to minimize collection. (Claerhout, 2005)

Generally speaking, the case studies presented in policy-based research take a fact based approach, without examining the ethics of privacy. Popp and Poindexter present a proposal for countering terrorism through information and privacy-protection technologies originally part of the DARPA research and development agenda as part of the Information Awareness Office (IAO) and the Total Information Awareness (TIA) program. These programs were respectively based on the hypothesis that the prevention of terrorism was based on the acquisition of information used to determine patterns of activity indicative of terrorist plots. This information is both collected and analyzed, and the authors proposed that privacy protections can and should be implemented as part of both of these activities. The paper provides quantitative data demonstrating that time spent on the analysis phase of intelligence activities can be exponentially increased using IT methods, which also eliminate ‘siloed’ information analysis (generally agreed to be one of the problems resulting in the failure to prevent the September 11 2001 attacks). However, the authors do not discuss the business purpose behind these programs – a critical legislated privacy requirement is the
justification for personal information collection - and / or question the factual evidence that supported the development of IAO and TIA.

Much of the work on assessments, including methodology and comparative analysis, was undertaken by legal scholars. Clarke’s work, for example, provides an excellent comparative overview of the use of PIAs in different jurisdictions, but is largely useless for providing input to formalization.

While assessments are a relatively well-researched topic in privacy (in particular outside the discipline of CS), there are few privacy breaches studies that go beyond incident rates. Linginal et al present a unique empirical study on the causality of privacy breaches based on the GEMS error typology. The authors conclusion is that different systems need to be built differently to mitigate the risk of human error.

Guarda and Zannoni are among few researchers who suggest an implementable model for engineering privacy requirements. Their paper introduces the field of “privacy engineering” to describe the current technical efforts to systematically embed privacy relevant legal primitives into technical design. Like the work on privacy ontologies (Hassan and Logrippo) in order to align the privacy artifacts, Guarda and Zannoni note that aligning enterprise goals with privacy policies, data protection policies and user preferences is key. The authors provide a unique contribution; however, the model is too complex to be implemented.

Venter et al’s paper on Privacy Intrusion Detection Systems (PIDS) is another unique contribution to the field. The authors propose a system for detecting privacy intrusions on a high level by detecting anomalous behaviour and reacting by throttling data access and / or issuing alerts using privacy enhancing technologies (PETs), including the Layered Privacy Architecture work that encompasses the personal control layer, organizational safeguards layers, private / confidential communication layer and the identity management layer. The PIDS (like traditional IDS models) is applied to an unauthorized query case study based on the assumption that information is stored in a central networked repository, and the results can be monitored and throttled depending on the anomaly profile feature. The authors themselves, however, note that the successful implementation of the PIDS depends on a PIDS anomaly profile for each subject derived from the subject’s role, including features, which is difficult.

While Guarda and Zannoni and Venter et al’s work focuses on infrastructure, the majority of scholars in this classification of research focus on specific implementations. Two of the more interesting examples are represented here in Clarkson et al, who present a technique for authenticating physical documents based on random, naturally occurring imperfections in paper texture and Jha et al who use genomic computation as a case study for developing a privacy-preserving implementation for computational biology. Where Clarkson’s focuses on how to authenticate the paper itself – not the content printed on a page – Jha et al’s work on DNA collection is an inherent threat to privacy.

The two researchers take oppositional approaches to protecting privacy by embedding it in design. Clarkson seeks to create a process which allows for registration and validation of the sheet of paper without a central registration authority, thereby minimizing privacy risk. On the other hand, Jha et al state that protecting the privacy of individual DNA when the corresponding genomic sequences is available is not realistic, so they choose to outline a practical tool to support collaborative analysis of genomic data without requiring release of underlying DNA and protein sequences. Since both allow for relatively easy re-identification, privacy protections are negligible.

While Guarda and Zannoni touch briefly on online privacy policies and user preferences, including the adoption of P3P and the P3P Preference Language (APPEL), privacy-aware access control languages, including E-P3P, EPAL and XACML; there are other researchers that have an in-depth focus on the use of these techniques for online privacy. Cranor et al study the deployment of the standard W3C platform for privacy preferences (P3P) format to assess usefulness to end users and researchers. The methodology for the study required the analysis of both machine-readable P3P policies and human-readable privacy policies; in order to assess both, Cranor et al utilized the Privacy Finder P3P evaluator and the W3C P3P Validator. The policy study also examined, as many researchers in this area do, the content of policies (including settings, marketing and sharing), industry trends (type of data collected, uses for data collected, data recipients) and popular sites.

There is a growing body of work on policy errors, semantic and syntactic, which Cranor et al contribute too in this work. Other researchers in the privacy policy online environment study the efficacy of P3P as a viable technology for privacy protection. Reay et al uniquely apply signal theory, and assess performance using traditional methods of signal theory analysis. Nonetheless, the predictions presented are not particularly surprising: P3P adoption will remain stagnant, little or no corrective maintenance on invalid P3P documents will be undertaken and little or no perfective maintenance will be undertaken on P3P policies because sellers are unmotivated.

The last two papers are part of many that propose applied techniques in social networking to address online privacy. Narayanana and Shmatikov present a methodology that demonstrates how anonymization techniques used by social network providers (Twitter, Flickr and LiveJournal) is easily undone with an error rate of 12%. Xiao and Varenhorst explicitly examine Twitter, and the inadvertent disclosure of personal information by end users because of general unawareness about the functionality of the service. Both researcher teams agree that anonymity is not a robust privacy-protection using real world examples that often involve releasing more information than necessary for re-identification, neither is it practical in social networking tools. In short, this type of research merely contributes to the loud call for privacy protection, but offers no solution.
IV. TRUST IN PRIVACY MODEL

Applying trust models to privacy assumes that formalization is a good thing, and the privacy can be treated similarly to trust; e.g. as a distributed system.

The purpose of formalization is to support the creation of a system to describe or model an idea. Formal models typically have their own languages – an agreed upon set of terminology that can be used to support the application of the model, but also debate and discussion about the model itself. In reviewing the previous section, it’s fairly evident that privacy as a discipline has failed to achieve even the primary objective of a common language. Given the rate at which technological advances continue to threaten informational privacy, it is definitely worth considering any new methods for advancing the cause.

Marsh notes that among other benefits, formalization – the creation of a trust model – may also be useful for other distributed systems. Distributed systems in computing reference multiple autonomous computers that communicate through a network. While informational privacy can be threatened in numerous ways, the online nature of communications is of paramount concern at the moment.7

A. One Proposed Model

Research on privacy and trust as linked phenomena remains scarce. Dwyer et al propose a “privacy trust model” in their paper based on a comparative analysis of Facebook and MySpace as outlined in Figure 1.

The proposed model is “a visualization of a theoretical model that guided data collection and analysis” for their study. “The independent variables are internet privacy concern, trust in the social networking site, and trust in other members of social networking sites.” (Dwyer, 2007) In the published results, the participants were asked to rate their feelings on two questions: (1) “I feel that the privacy of my personal information is protected …” and (2) “I trust that …”. As such, this is not a privacy trust model; primarily it fails to explicate the basic terminology. It is also not an operational privacy evaluation model.8

The model does, however, provide additional evidence for a scaled privacy measurement; although it is muddied somewhat by the misuse of the term ‘privacy’. Dwyer provides a comparative analysis of user perceptions of privacy and trust on Facebook versus MySpace (Dwyer, 2007). The study demonstrates that while members of both sites report similar privacy concern, Facebook members expressed significantly greater trust in both Facebook and were therefore willing to share more identifying information (emphasis added). In other words, the level of trust corresponded negatively to the level of privacy as defined by the authors; users trusted more so they disclosed more. This observation provides more evidence of the relationship between trust and privacy, and the need for formalized privacy model.

B. Trust in Privacy Model

Trust can be modeled in many different ways. The model itself can change the nature of the understanding. In applying the trust model to privacy, the same consideration exists. The proposed formalization for privacy is based on three considerations; outlining states of privacy, examining privacy based decision-making, and exploring the applicability of the agents as appropriate representations of people in the computational environment.

Privacy is described in legislation in explicit terms: personal information is subject to requirements, non-personal information is not.9 Legislation typically does not consider context or environment, e.g. where a piece of information may not be circumscribed as ‘personal information’ but an individual may consider it to be very personal information. For example, the physical location of my office may be non-personal information but if I am a victim of stalker, it may be very personal to me. Rather than computing the definition, a formalization of privacy should begin with the recognition that information types exist beyond those specifically identified in legislation, as proposed in Figure 2 below.

B. Trust in Privacy Model

Privacy is described in legislation in explicit terms: personal information is subject to requirements, non-personal information is not.9 Legislation typically does not consider context or environment, e.g. where a piece of information may not be circumscribed as ‘personal information’ but an individual may consider it to be very personal information. For example, the physical location of my office may be non-personal information but if I am a victim of stalker, it may be very personal to me. Rather than computing the definition, a formalization of privacy should begin with the recognition that information types exist beyond those specifically identified in legislation, as proposed in Figure 2 below.

Privacy is described in legislation in explicit terms: personal information is subject to requirements, non-personal information is not.9 Legislation typically does not consider context or environment, e.g. where a piece of information may not be circumscribed as ‘personal information’ but an individual may consider it to be very personal information. For example, the physical location of my office may be non-personal information but if I am a victim of stalker, it may be very personal to me. Rather than computing the definition, a formalization of privacy should begin with the recognition that information types exist beyond those specifically identified in legislation, as proposed in Figure 2 below.

7 Lessig stated that the lack of a record in social interactions is the passive enabler of privacy. Whether or not this is possible online is yet to be determined, but without re-architecting the Internet, this seems highly unlikely.

8 The stated objective of the study was to “compare(d) perceptions of trust and privacy concern”. Perhaps the theoretical model was mismnamed.

9 See, for example, Ontario’s Freedom of Information and Protection of Privacy Act, available online at [http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm](http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm). Personal information is defined in section 2.
Given that there are four different factors that provide input to an individual person’s privacy, privacy based decision making becomes fluid. Marsh’s model illustrates thresholds for trust that can be adapted to describe privacy decision-making, as in Figure 3.

![Figure 3: Proposed Thresholds for Privacy](image)

The rationale for the applicability of the model to privacy remains the same as Marsh describes for trust:

*Trust has a value which has no units, but can still be measured in terms of such vague notions as 'worthwhileness' and 'intrinsic value'. One either trusts, or one does not … this suggestion that trust has certain threshold values, above which it is possible to say that something or someone 'is trusted,' below which it is possible to say that is 'is not trusted.' (Marsh, 1994)*

Recent research has begun to examine privacy in a similar context; in particular, the return on investment that a company’s privacy program may have (Mulligan, 2008). Dating back as early as the 1970’s, researchers had begun to examine the economics associated with privacy, and the revelation that personal information exchanges involved tangible and intangible benefits for the giver (data subject) and receiver (data holder) (Acquisti, 2009, 2010).

Once the threshold has been established, the question becomes whether artificial agents can be utilized to represent privacy decision-making accurately. Agents, like those Marsh proposes to act on trust decisions, can also act for people to make decisions on privacy for the same reasons. First, artificial agents are assumed to be intelligent and rational. Privacy decision-making is a complex process that takes in to consideration beliefs and attitudes of individuals (Acquisti, 2009, 2010; Dwyer, 2007). The goal of course, is a scale for a rational privacy decision as represented on the proposed threshold in Figure 3. Third, agents are cooperative (Marsh, 1994), and primary learning from privacy decision making will be based on the outcomes of the interaction between data subject and data holder in disclosure of personal information (Acquisti, 2009, 2010). Fourth, the distributed nature of agents engenders the representation of social concepts (Marsh, 1994); in this respect privacy is particularly similar to trust as discussed in Section 2 of this paper. In addition, the independence of agents allows for thorough anomaly detection. Privacy agents in particular will require such detection given the established irregular patterns of decision-making that people demonstrate in personal information disclosure (Acquisti, 2010; Dwyer 2007).

V. CONCLUSION

Vampire bats need to eat 50-100% of their body weight in blood every night. If they fail to eat, they cannot maintain body temperature, critical to their survival. Hungry vampire bats groom other bats around the stomach area, eventually licking their faces to solicit food. If receptive, the donor bat will respond by regurgitating blood. This process of food sharing is a highly unusual characteristic in mammals; in theory, for it to work, bats cannot cheat – take blood, but not reciprocate. However, it has not yet been proved that cheaters exist or are excluded. In effect, the donation of blood is an altruistic act (Wilkinson, 1990). Like people when they decide to tell someone a secret, the vampire bats make a risk-based decision, and display trust (Marsh, 1994). This mammalian drive towards reciprocity needs to be replicated in the actions of artificial agents in order for the formalization to be implementable.

Future work will expand the proposed privacy formalization model. Additional details on the states of privacy will be explored, alongside the economics and rational theory under pining privacy decision-making to inform the applicability of the threshold in Figure 3. In addition, preliminary testing to inform learning of the artificial agent with an eye towards development accurate privacy agent representation will begin.

To some extent, the use of a trust model as a basis for formalizing privacy risks interpreting privacy as a technical standard for which some organization is responsible. This may be an improvement in the current complaint-driven approach to enforcement. In the event the model does not work, or privacy cannot be represented by agents, the work is beneficial in its contribution towards formalization of privacy by state identification and the establishment of thresholds.

ACKNOWLEDGMENT

This paper was completed with the support and guidance of Dr. Kahlil el-Khatib and Dr. Steve Marsh.

REFERENCES

[5] Claerhout, B and G. DeMoor. “Privacy Protection for Clinical and

---

10 The privacy legislation may in fact apply to these independent agents, an interesting consideration for implementation.


