Peer-produced Privacy Protection

Vaibhav Garg
Dept. of Computer Science
Drexel University
Philadelphia, PA
Email: gargv@drexel.edu

Sameer Patil
Helsinki Institute for Information Technology HIIT
Aalto University
00076 Aalto, Finland
Email: sameer.patil@hiit.fi

Apu Kapadia, L. Jean Camp
School of Informatics and Computing
Indiana University
Bloomington, IN 47408 USA
Email: {kapadia, ljcamp}@indiana.edu

***Abstract*— Privacy risks have been addressed through technical solutions such as Privacy-Enhancing Technologies (PETs) as well as regulatory measures including Do Not Track. These approaches are inherently limited as they are grounded in the paradigm of a rational end user who can determine, articulate, and manage consistent privacy preferences. This assumes that self-serving efforts to enact privacy preferences lead to socially optimal outcomes with regard to information sharing. We argue that this assumption typically does not hold true. Consequently, solutions to specific risks are developed — even mandated — without effective reduction in the overall harm of privacy breaches. We present a systematic framework to examine these limitations of current technical and policy solutions. To address the shortcomings of existing privacy solutions, we argue for considering information sharing to be transactions *within a community*. Outcomes of privacy management can be improved at a lower overall cost if peers, as a *community*, are empowered by appropriate technical and policy mechanisms. Designing for a community requires encouraging dialogue, enabling transparency, and supporting enforcement of community norms. We describe how peer production of privacy is possible through PETs that are grounded in the notion of information as a common-pool resource subject to community governance.**

I. Introduction

Technological advances in the past two decades, in software as well as hardware, have resulted in a great transformation in how we interact with other parties socially and commercially. While powerful computing devices, coupled with universally available Internet access, offer great benefits and conveniences, they also present a wide range of privacy risks and problems.

Typically, such privacy issues and concerns are tackled via technology or regulation or some combination of the two. The technical approach involves designing Privacy-Enhancing Technologies (PETs) that counter threats to privacy posed by the use of the underlying technology. For example, encryption and access control are PETs used to guard information from access by unauthorized parties. On the other hand, regulation utilizes measures such as guidelines, policies, contracts, and laws. These are used to describe uses and applications of technology that are *not* permitted, even when they are technologically feasible. For instance, it is easily possible to run face-detection algorithms on any given photograph. However, Facebook needed to disable such a feature in Europe in response to recent European Union regulatory actions.[1]

[1]Financial Times: Facebook ends facial recognition in Europe. http://www.ft.com/cms/s/0/fa9c4af8-03fc-11e2-b91b-00144feabdc0.html

While these two approaches mitigate and tackle various privacy aspects, one of their limitations is that they operate under the paradigm of individuals independently managing their own information. This paradigm involves several fundamental assumptions about individual decision making regarding privacy matters:

- The individual has correct and complete information to make a decision. For instance, privacy (control) settings assume that people have necessary and sufficient *a priori* information to specify preferences that will apply to *future* information sharing behaviors.
- The individual is able to articulate privacy needs. For instance, specification of privacy preferences requires explicit description of desires and needs that are often tacit and implicit.
- The individual is aware of the existence of PETs and privacy regulations. For instance, the onus and burden is often placed on privacy-conscious individuals to learn whether or not it is possible for the system to serve their privacy needs and whether the system provides mechanisms or policies for this purpose.
- The individual understands the user interfaces and interactions for managing privacy. For instance, it is generally assumed that users operate with correct understanding and mental models of how the underlying system operates and how various privacy options affect this operation.
- The individual is able to translate articulated privacy requirements into preferences that can be specified via the available interface and interaction mechanisms. For instance, users are tasked with translating their privacy needs as stated in natural language into a formal "specification" that the system can parse, process, and enforce.
- The individual is able to keep track of changes in privacy desires based on changes in context and, in turn, able to update privacy preferences such that they remain contextually appropriate. If privacy desires change due to a change in context, the individual must manually update privacy preferences to match the new privacy requirements.
- The individual makes privacy decisions that achieve his or her privacy desires in an optimal manner. For instance, privacy-related actions and behaviors of people are assumed to achieve their stated privacy goals.

Empirical research, however, has shown that these assumptions are often not met in practice. For example, individuals frequently make decisions with incomplete and/or inaccurate information [1], [2], may not fully understand how technology affects privacy [3], cannot completely and accurately describe their privacy needs [4], exhibit behavior inconsistent with their own stated privacy concerns [5], do not know about or utilize privacy management mechanisms [6], [7], [8], are confused by interfaces for specifying privacy preferences [9], [10], and find it difficult and burdensome to adjust preferences according to context [11].

A possible approach to address these issues is to develop techniques and solutions that attempt to eliminate, or minimize, the discrepancy between the ideal and practice. However, even if this ideal were achieved, the paradigm of an individual making decisions about privacy suffers from two additional shortcomings.

First, the individual decision-making paradigm assumes that individually optimal privacy decisions lead to privacy outcomes that are socially optimal (and desirable) for the community. However, prisoner's dilemma [12][2] and the tragedy of the commons [13][3] provide evidence of individually rational decisions that can lead to Nash equilibria that are suboptimal from a communal perspective. For instance, in the case of privacy an individual may perceive the risk of privacy violation not worth the cost of privacy protection. However, the information content of a database that aggregates individual pieces of information is greater than the sum of its components. Thus, risks for privacy violation for the database is arguably greater than the sum of privacy violation risks of each individual piece of information it contains. It is possible that the expected value of this aggregate privacy risk is greater than the aggregate cost. In hindsight, it may then be rational to have invested in privacy protection.

Second, the rational-individual paradigm ignores the role of the actions of others in affecting an individual's privacy, *independent of actions of the individual*. The social and professional relationships one maintains — online as well as offline — result in individual privacy being affected by actions of those with whom they are connected. For instance, even when an individual withholds his or her birthdate from the provider of an online Social Networking Service (SNS), birthday greetings of his or her friends via public (or private) messaging mechanisms of the SNS result in implicit disclosure of the birthdate to everyone (or at the very least the SNS provider).

We suggest that a fruitful way to address these shortcomings is to shift from the individual to a *community*-based approach. It has already been noted that information sharing typically takes into account an imagined community [8]. In fact, PETs have been criticized for ignoring trust among individuals in a community [14]. We address these limitations by considering privacy not as a public or a private good but a common-pool resource. Ostrom et al. note that successful and sustainable community-based governance of such a shared (common-pool) resource is contingent on five conditions [15]:

1) Monitoring the resource must be cheap.
2) The community must have a mechanism to maintain the reputation of the users of the resource.
3) The rate of change of the resource should be relatively constant.
4) It must be possible to exclude individuals from using the resource.
5) Community members must support the enforcement of community norms and therefore the monitoring required for effective enforcement.

These five conditions suggest that design for community governance requires encouraging dialogue between community members, enabling transparency of information flows, and supporting enforcement of community norms.

Ostrom et al. [15] acknowledge that in practice any given resource rarely meets all five conditions. However, institutional structures can be put in place to meet these requirements artificially without the construction of explicit property rights. For example, it may be difficult (i.e. expensive) to monitor if a fishery is being overfished. Then an alternative solution is monitoring and mandating the conduct of resource users through cooperatives of fishermen [16]. This is also true of community management of privacy in the online realm, where technical measures can complement or substitute institutional (or policy) measures. In this paper we discuss specific technical solutions that enable commons-based communal governance to achieve peer-produced privacy protection.

Section 2 begins by providing a description of Ostrom's framework. In Section 3 we discuss the limitations of current approaches. Further, we show how Ostrom's framework can be used for a systematic discovery of these limitations. Section 4 describes several technical solutions to peer-produced privacy protection grounded in Ostrom's notion of community-based governance of the information commons. Finally, Section 5 concludes with a discussion of future work.

II. A Common Pool Approach

As mentioned above, for successful governance of a common-pool resource through local stakeholders, the five conditions discussed below should be met:

A. Resource monitoring should be inexpensive.

This allows all stakeholders to be aware of how peers in their community are accessing and consuming the resource. In terms of privacy, this condition is rarely met. Even when

[2]Prisoner's dilemma refers to situations when two individuals, who cannot communicate directly with each other, must choose between cooperating or acting selfishly. The reward for selfishness is the highest *provided the other person does not act selfishly as well*. If both are selfish, they get no reward. However, if they choose to cooperate then each receives a reward, albeit lower than what would have been received by a single person acting selfishly. However, the combined reward of two cooperating individuals is greater than that of a single selfish person.

[3]Tragedy of the commons arises in the use of shared resources (e.g., oceans, parks, etc.). It is in the collective long-term interest of the group to protect the resource from depletion. However, the economically rational choice from the perspective of an *individual* member of the group is to maximize his or her resource consumption, leading to depletion of the resource.

information is shared willingly, it is almost impossible to observe the information flows post hoc. For example, even when Facebook controls are utilized adequately and information is shared with a specific person, there are limited, if any, options to know how frequently that information is being accessed by the specific individual.

Similarly, while Web sites differ in their privacy policies, there is little incentive for most of them to use privacy policy as a selling point. From a behavioral perspective, even a good faith discussion of the privacy policy could create anxiety for the consumer and deter adoption [17]. Users may, for example, express higher privacy concerns when primed [18]. Similarly, technical tools are rarely available to allow users to analyze how information about them is collected and distributed by different Web sites. Moreover, the tools available, such as Ghostery, do not allow users to pool information in a manner that enables discriminating among Web sites based on privacy.

B. Maintaining the reputation of resource users is essential.

The second requirement is that of social capital, i.e., those accessing the resource should have frequent face-to-face communication to establish trust. Face-to-face communication is not always possible on the Internet. However, technical substitutes like reputation systems can serve as a reasonable proxy for gauging social capital. However, such features have not yet been incorporated into common PETs. Existing solutions such as TRUSTe seals are not peer produced and suffer from incentive misalignment, i.e., their customers are Web sites and not the individuals whose privacy is to be protected [19]. Consequently, Web sites with such seals often provide less stringent privacy protection [20]. Peer production of reputation eliminates the cost of hidden action, as those generating the reputation rankings are also the ones interested in using the reputation information.

Peer-produced reputation systems, such as the Web of Trust plugin, are available for rating the information security of Web sites. However, similar reputation information regarding privacy policies and information collection/sharing behaviors of Web sites is not easily available [17] and it is often expensive for the user to be rationally indifferent [21].

C. The resource change rate should be relatively constant.

A third condition requires moderate rates of change, i.e., the resource, those using the resource, as well as the technological, social, and economic conditions surrounding the resource should not change too aggressively. It is hard to argue whether or not this is true for information commons. It is easier to examine whether this condition is relevant for online privacy.

For physical goods, moderate rates of change are required to enable monitoring and reputation. Arguably, if the number of individuals using a fishery changed frequently, social capital would be hard to compute. Similarly, if those using the resource change constantly, it would be difficult to monitor individual usage of the resource. This situation can, however, be addressed by increasing the cost of adding a resource consumer or the opportunity cost of losing an old one.

For physical goods, moderate rates of change of the resource are also needed for reasons of sustainability. If the rate of consumption of a resource were higher than the rate with which it can be replenished, then it would no longer be sustainable. This notion of sustainability is not relevant for information online.

However, in the case of privacy the cost of enforcing community norms could make peer governance unsustainable. Thus, it is important to consider the cost of enforcing community norms in comparison with those of enacting individual preferences. It has been argued that individuals have a limited security budget [22]. This would arguably be true for privacy as well, i.e., users would have a limited amount of resources that they would be willing to spend on achieving their privacy goals as well as enforcing community privacy norms. In peer-produced privacy protection, individuals select their peers, and therefore set the nature of community norms. Thus, compliance could arguably be higher making it possible to achieve privacy "sustainability."

D. Excluding individuals from resource use must be possible.

The fourth requirement refers to exclusion, i.e., it should be possible, and relatively inexpensive, to exclude entities from the resource. For physical resources this exclusion may be binary. For example, while members of a village on the riverbank may be allowed to fish in the river, those not from the village forbidden from doing so. Online, however, choices are rarely binary. Given the contextual nature of privacy, exclusion becomes problematic. For instance, an individual may want professional colleagues to get SNS status updates about new publications, but not about vacations. Location privacy is particularly problematic. Even for individuals with whom one is willing to share location information, one might be concerned if that information is accessed too frequently [23].

Exclusion has been a major focus of many PETs and privacy policies. Encryption, for example, excludes everyone other than those with access to the appropriate keys to decrypt the information. Similarly, privacy controls on Facebook prevent those without appropriate permissions from viewing information from an individual's profile. On the policy front, initiatives such as Do Not Track allow consumers to prevent Web sites from collecting information for tracking online behavior.

E. Community must support enforcement of norms.

The final requirement is that of enforcement, i.e., community members are able to identify when norms are violated and then penalize defectors through exclusion or other measures. For privacy, this is particularly difficult to achieve, especially with current controls. Privacy is contextual, however privacy preferences are typically provided a priori and out of context. For example, a user typically permits mobile applications to access location information ahead of time, before knowing whether an access may reveal information that he or she does not wish to share.

Simultaneously, the visibility of broken privacy norms is low. Ideally, when norms are broken, peers in a community

TABLE I
PROPERTIES OF GOODS

	Excludable	Non-excludable
Rivalrous	Private	Common pool
Non-rivalrous	Club/Toll	Public

can and do create pressure that leads to compliance. For example, the change in the intellectual property policy of Instagram upon acquisition by Facebook was perceived as breaking the foundational norm of the Instagram community, viz., photographs were not for commercial use. The resulting community backlash resulted in Facebook repealing the policy change.[4]

Successful governance of the information commons by peers to prevent privacy violations requires that all five requirements above be met. Yet, existing technologies provide only a subset of these requirements. It is also important to note that these five requirements are often interdependent. For example, if monitoring is either not possible or prohibitively expensive, enforcement would be unlikely to happen in practice even if enforcement mechanisms were readily available. Thus, partial fulfillment of these requirements with regards to the information commons may create the illusion of risk reduction without an actual decrease in the overall harm of privacy breaches.

III. CURRENT APPROACHES AND THEIR LIMITATIONS

Economic theory categorizes goods into four types: public, private, common pool, and club. The categorization is based on whether a good is excludable and/or rivalrous (see Table I). If individual entities can be prevented from consuming a resource it is excludable. The good is rivalrous if it can be subtracted, i.e., one individual's consumption of a good leaves less of that good for others. These properties are often mutable.

Canonical wisdom states that systems are sustainable, but only under a paradigm that considers system resources to be either a public or a private good. The notion of privacy as *confidentiality* considers information as a private good. When information is considered a private good, the assumption is that information about a specific person is only relevant to them; information sharing by that person then puts only that specific individual at risk. Thus, solutions have focused on encryption technologies.

However, this assumption fails often in real life. For example, public records of genomic information about an individual are relevant to both the primary stakeholder and his or her relatives. In fact property rights over certain kinds of information can be hard to assign. For example, when a group photograph is taken at a party, it is ambiguous who among the group has the right to post the picture online. Assigning the rights to the person who takes the photograph or to the owner of the camera may lead to privacy violations.

[4]The Washington Post: Instagram, Facebook stir online protests with privacy policy change. http://articles.washingtonpost.com/2012-12-18/business/35908189_1_kevin-systrom-instagram-consumer-privacy

A second argument considers information to be public good. Posner argues that given that information makes markets more efficient only those involved in unsavory activities would be invested in hiding information, i.e., privacy is valuable only to those who have something to hide [24]. Even Posner, however, did not assume that information should be freely available. For markets to be truly efficient the individual whose information is being used should be reimbursed for that resource [25]. Therein lies the idea of privacy as control; information sharing is enabled only when both parties involved have higher individual utilities after the transaction takes place. Information as a public good paradigm is used to develop policy solutions such as Do Not Track; the individual can choose to be tracked if the transaction is mutually beneficial or if privacy loss is adequately reimbursed by the benefits of targeted advertising derived from behavioral tracking.

On the technical side, control is enabled by PETs that assume a rational end user who can manage privacy preferences to achieve optimally effective information flows. As described before, this assumption of rationality is problematic.

These and other criticisms of PETs have been made in prior literature [14]. Here we discuss two additional limitations of existing paradigms. First, solutions to privacy risks target individuals. The narrow perspective of the rationality assumption then presumes that individually rational decisions would lead to socially optimal (or even socially desirable) outcomes. This is often false as many privacy risks are not controlled fully by individual actions but arise from aggregation of actions of the many. For instance, in the case of targeted advertising, even when an individual chooses not to be a part of a database, inferences can still be made about him or her based on the aggregate inputs of other participants. Moreover, the refusal to be tracked is revealing in its own sense.

A second limitation of the rational actor paradigm of the end-user is that of costs. However it has been shown that individually rational decisions often lead to suboptimal Nash equilibria, e.g., prisoner's dilemma and on a larger scale tragedy of the commons [13]. The problem is further compounded for privacy. For a single individual the perceived costs of implementing PETs may be perceived as high, while those of privacy infringement may be perceived to be low. However, as described above, an information database is greater than the sum of its parts. Thus, the aggregate privacy loss — for the individual as well as the community as a whole — may be greater. Arguably, then, voluntary information disclosure can be characterized as a tragedy of the information commons.

The typical approach to addressing the tragedy of the commons has been through public or private interventions. Let us consider private interventions first. Arguably, there are (academic) incentives for private parties to preserve the common-pool or community resources both offline and online. In the offline case, it is in the interest of the private entity to sustain the community resource, such as a fishery or a forest, for long-term gain. Incentives to provide stronger online PETs have been noted both from a rational choice [26] and behavioral perspective [27]. In practice, however, the

destruction of natural resources owned by private entities is widely documented and reported [28], while the lack of usable and useful controls for online privacy often does not receive the same level of attention. Similarly, providing privacy information through private entities such as TRUSTe seals creates a only a perception of increased privacy, which may in fact lower protection due to the resulting incorrect risk compensation. (In fact it has been noted that such perception could result in more risk taking behavior [27].)

To overcome these shortcomings, a second approach that is being tried is public interventions through the Federal Trade Commission (FTC), e.g., Do Not Track. Despite good underlying intentions, such interventions have had limited success in the offline realm. A key constraint is that public officials often have limited knowledge about the resource, such as fisheries, compared to the granular information available to locals who are invested in sustaining the ecosystem due to the economic security it provides in the long term. For example, public efforts have managed to preserve local forests while simultaneously destroying the diversity of flora and fauna due to limited knowledge of the ecosystem [29].

A third possibility is that of considering information as a commons that is best managed by those adversely effected by a privacy breach. As noted in the previous section, five requirements must be met for such an approach to be successful: monitoring, reputation, moderate rates of change, exclusion, and enforcement. This five-dimensional framework can be used to identify the failures of current privacy solutions. We can take the example of Facebook privacy controls. Currently, these controls do not allow monitoring. For instance, it is not possible for individuals to ascertain if and when their information is being accessed by their peers (i.e., Facebook friends). On the other hand the social network Orkut did provide such functionality. Specifically, users could opt-in to be able to view the last five individuals who visited their profile. However, this also meant that when they visited someone else's profile that visit would be disclosed to the other individual.

Facebook provides no mechanism to establish reputation; a user cannot identify if certain peers excessively or inappropriately tend to access his or her information or post information about him or her. It may be that a member of an individual's friend circle repeatedly post pictures in which he or she tags the individual. These pictures and the related tagging may be undesirable to that individual. However, the individual is burdened with removing each tag individually. If there were mechanisms to influence the "reputation" of peers, one could provide feedback to the offending member, who may then consider changing his or her behavior or risk having a poor reputation. The feedback could also be displayed to the peer community, who would then be aware of the offending individual's deviance from the norm.

In terms of "rates of change," Facebook often changes both the interface and the functionality of its privacy controls. Yet, advances in privacy controls are generally much slower than the increasing pace of automation of information sharing (for instance, Facebook can now tag individuals in photos based on automatic face recognition). In terms of peers, the turnover rate is dependent on the users themselves, and individuals can choose to increase or decrease the number of peers they are connected to at any time.

A limited form of exclusion is possible on Facebook. Users can choose to exclude peers that they feel should not have access to their information. However, excluding Facebook itself is not an option (unless one chooses to disclose information *outside* the Facebook platform entirely). Another key issue is the "right to be forgotten" [30]. Facebook does not allow users to delete their information if they so choose. Thus, Facebook can only be excluded from future data and not past data. (The social network Google Plus does allow users to remove their data from Google servers if they choose.)

Enforcement on Facebook is possible to a limited degree; it is possible to be friends with a certain individual as well as to increase or decrease his or her privilege based on whether he or she appears to be following a given norm. Unfortunately, as noted before, due to lack of transparency, it is unclear if someone breaks a norm. Ideally, it should be possible to utilize a norm itself as an aspect of privacy control; those that follow the norm would be allowed access to the information in question while deviations from the norm will result in curtailed access not only to at the individual level but also at the community level.

The above discussion highlights how Ostrom's framework can be used to examine the limitations of current solutions for privacy protection, especially when those solutions impinge on community-based governance of the information commons. In the next section we present existing research that argues for self-governance of the information commons and the technical solutions that enable such communities.

IV. Peer based Approaches in Technical Implementation

Privacy functionalities in technologies, in both the consumer and the interpersonal domain, have utilized approaches that include actions of parties other than the individual whose privacy is to be managed. These other parties — peers from the community — aid privacy management in a variety of capacities. Here we discuss a model of how privacy protection can be achieved by complementary design of technology and policy.

First is the notion of *norms* often instantiated via self-regulation to preserve one's role in a community. Although technology often enables violations of privacy, the social context in which the technology is embedded can act as a strong counteracting force due to prevailing norms about acceptable behavior. Due to the social costs of breaching these norms, peers in a trusted community are generally relied upon to regulate their own behavior such that it does not violate the privacy of others. As Dourish [31] notes regarding such 'cultural' models of privacy protection in the Media Space at Xerox PARC, "[w]ithin a small community, the result is a stable situation, comfortable and acceptable to participants,

without direct need for a more technological solution." This assertion suggests that the approach defined by Ostrom could apply to privacy management, even in a domain where levels of expertise are quite high.

Unfortunately, social norms without technological solutions often do not scale. As communities become larger, the cost of monitoring through non-technological means becomes prohibitively expensive. Technology could itself facilitate monitoring of privacy violations. An example of such functionality is feedback regarding "information exposure" [23], [32], [33]. *Information exposure* refers to actual accesses that occur within the permissible bounds specified by privacy settings. Exposure feedback serves as an indicator of how entities in a community — individuals, businesses, or the government — are consuming information. Such mechanisms lower the *cost of monitoring* privacy violations through increased transparency and allow community members to assess whether information accesses violate community norms. Exposure also enables assessing the reputation of peers based on the monitoring of their information consumption. Further, community members could act as "guardians," and respond to undesirable exposure patterns of individuals in the community.

For example, Bob may notice that Alice's Facebook status message is attracting more attention than was anticipated and can temporarily restrict access to that information (until Alice is able to assess her exposure). In such scenarios it is important to exclude undesirable people from the community. Indeed, excludability in the community of peers is the difference between privacy and censorship in the presence of guardians. Exposure norms can be effective only if there is control over data diffusion and the ability to remove information.

Research has also shown that those who are less technically savvy often rely on technical assistance from their social networks [34], [35], [36], [37]. Such assistance covers privacy affecting matters, such as configuring home networks, protecting against spyware, and setting privacy preferences. All three of these examples are domains where effective peer sharing of technological expertise could facilitate empowerment of the entire community. An individual can use information regarding aggregate community choices as guidance for making decisions. Such "social navigation" [38] approaches have been applied to inform decisions about cookie management [39], firewall rules [40], phishing sites [41], information access policies for Facebook applications [42], and privacy preference settings in Instant Messengers [43].

Here too, it is important that the consequences of shared privacy settings are communicated to the community. Transparency using an exposure-feedback approach could convey how these settings affect the privacy of the community. Reputation mechanisms could further track which community members provide more effective and useful controls.

In all of the above cases, a person relies upon and/or utilizes the actions of others from the community to enable more enhanced and effective protection of his or her privacy.

V. Future Work and Conclusion

Designing for a community that considers information sharing as a norm and PETs as covenants [44] is a profoundly different paradigm than one where individuals manage their own information. A community approach to privacy assumes existence of a group of individuals who share the risk of information sharing such that no one individual can assert complete privacy. Thus, peer protection recognizes information, and therefore privacy, as a common-pool resource.

Understanding privacy as a community good, but one that requires transparency and excludability for protection, has implications for regulation as well as technology design. The FTC has played a crucial role in ensuring that organizations comply with their privacy policies for individuals. A natural extension of the framework for peer protection would require that individuals be more empowered to limit and even remove information. Much of the technology for information control is extant; for instance, facial recognition is used to suggest tags on Facebook. However, it could just as easily be used to request permission from a person about public availability of his or her image before allowing another person to post it. In the absence of such technological support, relying only on norms has proven incapable of preventing unauthorized posting of photographs. A peer-centered approach would allow individuals to advise and support each other in their interactions and enable removal of digital tracks when desired. This would be an expansion of the current transactional approach to privacy. It retains the focus on transparency and expands it to include excludability of resources, construction of community, removal of data, and reduction of harm.

Privacy functionalities in technologies, in the consumer as well as the interpersonal domain, can benefit from utilizing approaches that include actions of parties other than the individual whose privacy is managed. These other parties — peers from the community — aid privacy management in a variety of capacities. Future work should examine policy instantiations that enable effective and sustainable community governance for privacy matters. Technology and policy should be treated as both supplements and complements to enable peer-produced privacy protection.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Award Nos. CNS-1016603, CNS-1228364 and CNS-1250367, Intel through the Intel Science and Technology Center (ISTC) for Secure Computing, and US DHS grant no. 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P). The contents of this paper do not necessarily reflect the views of the sponsors. We acknowledge the editorial help of John McCurley and Sara E. Justinger.

References

[1] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *Security & Privacy, IEEE*, vol. 3, no. 1, pp. 26–33, Jan.-Feb. 2005.

[2] S. Lederer, I. Hong, K. Dey, and A. Landay, "Personal privacy through understanding and action: Five pitfalls for designers," *Personal Ubiquitous Computing*, vol. 8, no. 6, pp. 440–454, Nov. 2004.

[3] S. Patil and A. Kobsa, "Uncovering privacy attitudes and practices in instant messaging," in *Proceedings of the 2005 International ACM SIGGROUP Conference on Supporting Group Work (GROUP)*. New York, NY, USA: ACM, 2005, pp. 109–112.

[4] S. Patil, Y. L. Gall, A. J. Lee, , and A. Kapadia, "My privacy policy: Exploring end-user specification of free-form location access rules," in *Proceedings of the Workshop on Usable Security (USEC)*, vol. 7398. Springer Berlin / Heidelberg, Feb. 2012, pp. 86–97.

[5] S. Spiekermann, J. Grossklags, and B. Berendt, "E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior," in *Proceedings of the 3rd ACM Conference on Electronic Commerce*. New York, NY, USA: ACM, 2001, pp. 38–47.

[6] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing Facebook privacy settings: User expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM Internet Measurement Conference*. New York, NY, USA: ACM, 2011, pp. 61–70.

[7] Consumer Reports Magazine, "Facebook & your privacy: Who sees the data you share on the biggest social network?" June 2012. [Online]. Available: http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm

[8] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in *Privacy Enhancing Technologies*. Springer, 2006, pp. 36–58.

[9] T. Paul, D. Puscher, and T. Strufe, "Improving the usability of privacy settings in Facebook," *arXiv preprint arXiv:1109.6046*, 2011.

[10] K. Strater and H. R. Lipford, "Strategies and struggles with privacy in an online social networking community," in *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction – Volume 1*. Swinton, UK, UK: British Computer Society, 2008, pp. 111–119.

[11] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in *Proceedings of the 19th International Conference on World Wide Web (WWW)*. New York, NY, USA: ACM, 2010, pp. 351–360.

[12] D. M. Kreps, P. Milgrom, J. Roberts, and R. Wilson, "Rational cooperation in the finitely repeated prisoners' dilemma," *Journal of Economic theory*, vol. 27, no. 2, pp. 245–252, 1982.

[13] G. Hardin, "Tragedy of the commons," *Science*, vol. 162, no. 3859, pp. 1243–1248, 1968.

[14] S. Gürses and B. Berendt, "PETs in the surveillance society: A critical review of the potentials and limitations of the privacy as confidentiality paradigm," in *Data Protection in a Profiled World*, S. Gutwirth, Y. Poullet, and P. De Hert, Eds. Springer Netherlands, 2010, pp. 301–321.

[15] E. Ostrom, *Governing the commons: The evolution of institutions for collective action*. Cambridge university press, 1990.

[16] F. Berkes, D. Feeny, B. J. McCay, and J. M. Acheson, "The benefits of the commons," *Nature*, vol. 340, no. 6229, pp. 91–93, 1989.

[17] J. Bonneau and S. Preibusch, "The privacy jungle:on the market for data protection in social networks," in *Economics of Information Security and Privacy*, T. Moore, D. Pym, and C. Ioannidis, Eds. Springer US, 2010, pp. 121–167. [Online]. Available: http://dx.doi.org/10.1007/978-1-4419-6967-5_8

[18] J. Gideon, L. Cranor, S. Egelman, and A. Acquisti, "Power strips, prophylactics, and privacy, oh my!" in *Proceedings of the second symposium on Usable privacy and security*, ser. SOUPS '06. New York, NY, USA: ACM, 2006, pp. 133–144. [Online]. Available: http://doi.acm.org/10.1145/1143120.1143137

[19] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 5799, pp. 610–613, 2006.

[20] B. Edelman, "Adverse selection in online "trust" certifications," in *Fifth workshop on the economics of information security*, 2006, pp. 26–28.

[21] A. McDonald and L. Cranor, "The cost of reading privacy policies," *ISJLP*, vol. 4, p. 543, 2008.

[22] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proceedings of the 2008 workshop on New security paradigms*, ser. NSPW '08. New York, NY, USA: ACM, 2008, pp. 47–58. [Online]. Available: http://doi.acm.org/10.1145/1595676.1595684

[23] R. Schlegel, A. Kapadia, and A. J. Lee, "Eyeing your exposure: Quantifying and controlling information sharing for improved privacy," in *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS)*. New York, NY, USA: ACM, Jul. 2011, pp. 14:1–14:14.

[24] R. Posner, "The right of privacy," *Georgia Law Review*, vol. 12, no. 3, pp. 393–422, 1977.

[25] ——, "The economics of privacy," *The American Economic Review*, vol. 71, no. 2, pp. 405–409, 1981.

[26] R. Böhme, S. Koble, and T. Dresden, "On the viability of privacy-enhancing technologies in a self-regulated business-to-consumer market: Will privacy remain a luxury good," in *Workshop on the Economics of Information Security (WEIS)*. Pittsburgh, PA: Carnegie Mellon University, 2007.

[27] L. Brandimarte, A. Acquisti, and G. Loewenstein, "Misplaced confidences: Privacy and the control paradox," *Social Psychological and Personality Science*, 2012.

[28] F. Berkes, "Fishermen and 'the tragedy of the commons'," *Environmental Conservation*, vol. 12, no. 03, pp. 199–206, September 1985.

[29] W. Ascher, "Communities and sustainable forestry in de-

veloping countries," Duke University, Tech. Rep., 1995.

[30] J. Rosen, "The right to be forgotten," *Stanford Law Review Online*, vol. 64, p. 88, 2012.

[31] P. Dourish, "Culture and control in a media space," in *Proceedings of the third European Conference on Computer-Supported Cooperative Work (ECSCW)*. Kluwer Academic Publishers, 1993, pp. 125–137.

[32] S. Patil and A. Kapadia, "Are you exposed? conveying information exposure (extended abstract)," in *Proceedings of The 2012 ACM Conference on Computer Supported Cooperative Work Companion (CSCW)*, Feb. 2012, pp. 191–194.

[33] Y. L. Gall, A. J. Lee, and A. Kapadia, "PlexC: A policy language for exposure control," in *Proceedings of The 17th ACM Symposium on Access Control Models and Technologies (SACMAT)*, Jun. 2012, pp. 219–228.

[34] S. Kiesler, B. Zdaniuk, V. Lundmark, and R. Kraut, "Troubles with the Internet: The dynamics of help at home," *Human Computer Interaction*, vol. 15, no. 4, pp. 323–351, Dec. 2000.

[35] E. S. Poole, M. Chetty, R. E. Grinter, and W. K. Edwards, "More than meets the eye: Transforming the user experience of home network management," in *Proceedings of the 7th ACM conference on Designing Interactive Systems (DIS)*. New York, NY, USA: ACM, 2008, pp. 455–464.

[36] E. S. Poole, M. Chetty, T. Morgan, R. E. Grinter, and W. K. Edwards, "Computer help at home: Methods and motivations for informal technical support," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. New York, NY, USA: ACM, 2009, pp. 739–748.

[37] L. J. Camp, "Reliable, usable signaling to defeat masquerade attacks," in *Workshop on the Economics of Information Security (WEIS)*, Cambridge, UK, Jun. 2006.

[38] A. Dieberger, P. Dourish, K. Höök, P. Resnick, and A. Wexelblat, "Social navigation: Techniques for building more usable systems," *Interactions*, vol. 7, no. 6, pp. 36–45, Nov. 2000.

[39] J. Goecks and E. Mynatt, "Supporting privacy management via community experience and expertise," *Communities and Technologies*, pp. 397–417, 2005.

[40] J. Goecks, W. K. Edwards, and E. D. Mynatt, "Challenges in supporting end-user privacy and security management with social navigation," in *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS)*. New York, NY, USA: ACM, 2009, pp. 5:1–5:12.

[41] T. Moore and R. Clayton, "Evaluating the wisdom of crowds in assessing phishing websites," in *Financial Cryptography*, G. Tsudik, Ed., vol. 5143. Springer, 2008, pp. 16–30.

[42] A. Besmer, J. Watson, and H. R. Lipford, "The impact of social navigation on privacy policy configuration," in *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS)*. New York, NY, USA: ACM, 2010, pp. 7:1–7:10. [Online]. Available: http://doi.acm.org/10.1145/1837110.1837120

[43] S. Patil, X. Page, and A. Kobsa, "With a little help from my friends: Can social navigation inform interpersonal privacy preferences?" in *Proceedings of the ACM 2011 conference on Computer Supported Cooperative Work (CSCW)*. New York, NY, USA: ACM, 2011, pp. 391–394.

[44] E. Ostrom, J. Walker, and R. Gardner, "Covenants with and without a sword: Self-governance is possible," *The American Political Science Review*, vol. 86, no. 2, pp. 404–417, 1992.