
A Community-Based Approach to Networked Privacy

Eran Toch

Tel Aviv University
Tel Aviv, 6997801, Israel
erant@tau.ac.il

Abstract

This short paper discusses the legitimacy of paternalistic privacy approaches that aim to nudge users to more privacy-oriented behavior in networks. I demonstrate that traditional theories for privacy, rooted in individualistic values, fail to justify paternalistic views. In response, I suggest tying networked privacy to community-based approaches that point to the importance of privacy in the process of establishing and maintaining a community.

Author Keywords

Privacy, social networks, positive liberty, communitarian philosophy, social penetration

ACM Classification Keywords

K.4.1 [Computers and Society - Public Policy Issues]: Privacy

Introduction

A few years ago I gave a talk at a startup meetup, organized by Microsoft R&D. I was talking about the privacy challenges related to creating a new tech company and presented Facebook as a case study. However, one particular audience member had insistently interjected to argue that there cannot be any privacy challenges in Facebook because users are free to choose what information they share. I pointed to the biases in Facebook's choice archi-

Negative and Positive Liberty

Political liberalism tends to pre-suppose a negative definition of freedom: liberals generally claim that if one favors individual liberty one should place strong limitations on the activities of the state, companies, and other agents that hold power over the individual.

In positive liberty, as defined by Isaiah Berlin [2], a person is free if she is self-determined, which is to say that she must be able to control her own destiny in her own interests. In positive liberty, we ask for the presence of something (i.e. of control, self-mastery, self-determination or self-realization), rather than the absence of external limitations.

ecture, but he insisted that any choice architecture will be arbitrary and that a promoting privacy is merely a political choice. At that time, I could not provide a better answer which was not a normative one. In this short position paper, I tried to put into words some initial ideas I had about a possible answer to the question that that nameless engineer had asked me.

The liberal theories that provide the foundation for today's legal frameworks treat privacy as an essential part of the individual's liberty. Theories such as the ones by Warren and Brandeis [10] and Westin's privacy as control [11], suggest to put bounds on the ability of powerful entities to restrict the individual's freedom. Arguably, this shared understanding was always contested, and it seems to be dwindling as new technologies redefine the relation between people and their information. In networked environments, a normative approach towards privacy, in which privacy is unequivocally "better" or "worse", requires agreeing on a standard set of values. In networked environments, the subjects of this paper, privacy processes mitigate information sharing and interactions between peers. As a result, the discussion is even more complicated. The interest of different peers can often be conflicted: a family member, for example, might want to share information about a more secretive member. Also, group interests can be inherently different than the values of specific individuals. For example, gossip can tie communities together, but can also offend particular individuals [8].

Applying libertarian ideas of privacy to networked environments is difficult. When analyzing social media and other networked scenarios with traditional ideas of privacy, the analysis leads scholars to point to seeming paradoxes [5]. Recent engineering approaches that aim to increase the level of privacy in networked environments do that by try-

ing to stir users to more privacy-oriented behaviors. Several works seek to change the way users make decisions about sharing information with their peers, through nudging [9], personalization of choice architectures [6] or peer pressure [7]. These efforts represent a *paternalistic privacy view* that assumes the normative place of privacy in networked environments, through ways to manipulate the behavior of users, and look at privacy as a default value (my work [7] included). To discuss the possible justifications for this view, I will discuss the shortcoming of existing privacy theories in justifying networked privacy. Then, I will suggest justifying paternalistic privacy by thinking about communities and individuals at the same time through social penetration theory.

Privacy and Liberty

The place of liberty in networked privacy is not unchallenged. We cannot assume that the user needs special protection from an all powerful entity like the state or a large corporation, as we expect some level of equality between peers. Moreover, paternalistic privacy is extremely challenging to be justified in a liberal and individualistic framework of thought. If the user is free to share everything, introducing any bias through regulatory processes is problematic. However, liberal theories look at privacy as a negative liberty, restricting the powerful entities, so that the individual could be free (see the sidebar on page 2 to read about negative versus positive liberty). On the other hand, to talk about positive liberty in a meaningful way, we need to put it in the context of something positive to be achieved. In its political form, positive freedom has often been thought of as necessarily obtained through a collectivity. Perhaps the clearest case is that of Rousseau's theory of freedom, in which people achieve freedom through participation in the process whereby one's community exercises collective control over its own affairs.

Communitarianism

Communitarianism is a philosophy that criticizes the deterioration of the community in response to the rise of capitalist mindsets, and advocates for the creation of stronger communities that are more reflective and responsive to the needs of society, as once individuals are collectivized into their communities, the citizens are more apt to act in responsible ways.

The sociologist Amitai Etzioni defined communities as having two characteristics: first, a web of affect-laden relationships among a group of individuals, relationships that often crisscross and reinforce one another and a measure of commitment to a set of shared values, norms, and meanings, and a shared history and identity [3].

What would positive liberty in networked privacy? What should be the content of a positive freedom of a user? One possibility is to think of the network as the equivalent of a community. In the case of a social network, we can think of community-driven objectives: to increase the social capital of each participant at the network and the ability of each to exercise free will in the network.

Between Communities and Individuals

In his book, “The Limits of Privacy” the communitarian sociologist Amitai Etzioni launches an attack on the way personal privacy in America [4]. Etzioni claims that privacy has become a “privileged right”, to the extent that it trumps all other rights. For communitarians (see sidebar on page 3), all rights are subject to reasonable limitations in the interest of other rights of equal or greater value and the common good. Etzioni provides guidelines to what should be the limits on privacy rights: how much, in what circumstances, and with what safeguards. The book suggested an updated, communitarian concept of privacy: a privacy that is not absolute but varies with context.

Etzioni’s attack on privacy is arguably one of the most serious ones, as it balances the interest of individuals with their interests as members of a community. This tradeoff is more challenging to privacy advocates than other tradeoffs in privacy, such as the ones between commercial interests and individualistic interests in social networks [5]. Moreover, the communitarian approach to privacy better extends to cultures outside of the United States, cultures that put less emphasis on the individual and more on the community. Personally, Etzioni’s language can portray situations and aspects that are familiar with my personal Israeli culture, values which are missing from individualistic views of privacy. As more and more American social platforms go international, we need theories that can reflect the place of

both individuals and communities in the technology. At the same time, Etzioni’s overlooks the principal place of privacy in communities.

Communitarian theories describe privacy as an interest of the individual, which is contrasted with the interests and values of the community, such as security, safety, and trust. However, this view disregards the importance of privacy in the process of building and maintaining healthy communities. Studies in social networks have shown that privacy can have a positive association with social capital [] and that the use of privacy controls can lead to stronger ties between users [12]. The theory of social penetration provides a compelling explanation for this phenomenon (see the explanation of the social penetration theory in the sidebar on page 4). When applied to social networks, we can expect that without mechanisms for managing privacy, relationships would not be able to grow, and as a result, the community itself could not develop properly. Social penetration theory tells us that people need to use discriminating information-sharing mechanisms, mechanisms that allow us to share differently with different groups.

Privacy in the Community

If we choose to value the community itself, the ability of the network to provide a place to establish connections and to accumulate social capital, then we can look at privacy as a value that serves both the community and the individual. In particular, when we try to evaluate paternalistic privacy mechanisms, we can judge them according to values that benefit the community and values that benefit the individual. From positive liberty, we put responsibility on the shoulders of users and network designers to cultivate and care for the network. Mechanisms that promote those values will promote social capital, social trust and self-actualization to its users.

Social Penetration Theory

The social penetration theory proposes that as relationships develop, interpersonal communication moves from relatively shallow, non-intimate levels to deeper, more intimate ones. The theory was developed by psychologists Irwin Altman and Dalmis Taylor in 1973 [1]. They describe a process in which relationships develop primarily through self-disclosure, or intentionally revealing personal information such as personal motives or desires, feelings, thoughts, and experiences to others.

The way norms of information sharing are formed and changed over time in a particular network can help us think of a normative approach that avoids the paternalistic approach. A useful mechanism provides users with the ability to establish their norms as a community, where people learn about behaviors and values from each other, forming their community-based informational norms which are unique to their particular situation. What can we expect from privacy mechanisms in these systems? They should provide enough freedom to users to experiment and change their behavior with time and context. They should be able to allow users to undo their decisions in some respect. They should provide some visibility into how users are managing their privacy to achieve learning between users. Do paternalistic privacy nudges accomplish these goals? We do not know yet. However, to some extent, they provide a way for users to think and evaluate their interests and behavior when sharing information.

References

- [1] Irwin Altman and Dalmis Taylor. 1973. Social penetration theory. *New York: Holt, Rinehart - Mnston* (1973).
- [2] Isaiah Berlin. 1969. *Four essays on liberty*. Oxford University Press.
- [3] Amitai Etzioni. 1994. *Spirit of community*. Simon and Schuster.
- [4] Amitai Etzioni. 2008. *The limits of privacy*. Basic Books.
- [5] Ralph Gross and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. ACM, 71–80.
- [6] Alfred Kobsa, Hichang Cho, and Bart P Knijnenburg. 2016. The effect of personalization provider characteristics on privacy attitudes and behaviors: An Elaboration Likelihood Model approach. *Journal of the Association for Information Science and Technology* (2016).
- [7] Tamir Mendel and Eran Toch. 2017. Susceptibility to Social Influence of Privacy Behaviors: Peer versus Authoritative Sources. In *ACM 2016 Conference on Computer Supported Cooperative Work, CSCW*.
- [8] Zeynep Tufekci. 2008. Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate? *Information, Communication & Society* 11, 4 (2008), 544–564.
- [9] Yang Wang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. 2013. Privacy nudges for social media: an exploratory Facebook study. In *WWW*. 763–770.
- [10] Samuel D Warren and Louis D Brandeis. 1890. The right to privacy. *Harvard law review* (1890), 193–220.
- [11] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.
- [12] Pamela Wisniewski, AKM Islam, Bart P Knijnenburg, and Sameer Patil. 2015. Give social network users the privacy they want. In *CSCW*. ACM, 1427–1441.