The appropriation of privacy: Policies and practices of everyday technology use

Jan Fernback
Undrah Baasanjav
Temple University
USA
fernback@temple.edu

Michael Zimmer
University of Wisconsin – Milwaukee
USA
zimmerm@uwm.edu

Kelly Quinn
University of Illinois at Chicago
USA
kquinn8@uic.edu

Alice Marwick
Fordham University
USA
amarwick@fordham.edu

Abstract

Privacy is a complex concept involving dimensions of access and control of shared information, expectations of intended audience, and appreciation of the context in which a communication takes place. As new technologies are introduced and become ubiquitous, they intersect with influences of culture and experience to influence and appropriate privacy's interpretation and meaning. This panel will explore how conceptions of privacy are shaped and understood by examining the implications that everyday technologies, and the policies and practices embodied therein, hold for the realization of privacy goals. Culture, mobility and utility of new media forms challenge the conception and construction of privacy in these multiple contexts, and these in turn seize and shape our sociability and interactions with others.

Intensely cultural, conceptions of privacy highlight the dialectical tensions between public/private and individual/community. Cultural conceptions of privacy inform, are reproduced and embodied in societal norms and political frameworks, and not only impact the individual in physical ways, but also as the body is digitized in communicative acts. Our first presenter will present findings of how mass media in China reproduce the ideological individual/community tensions that surface through the use of human flesh search engines, and how this is embodied in policy and political frameworks. Without clear privacy laws, the Chinese state may easily appropriate the concept of privacy away from the legal terrain of information control or human dignity and toward individual selfishness and shame.

Our second presenter will introduce the emerging infrastructures of augmented mobility technologies, and critically interrogate their impact on conceptions – and expectations – of privacy in our infosphere. Emerging augmented mobility platforms are wearable devices that promise to provide new ways of conceiving of our world through the layering of locational information and real-time informational objects onto a physical environment. Location-aware mobile Internet applications provide new layers of information to aid in navigation, decision-making, and social interactions. But they also require widespread tracking, collecting, and aggregating of users' precise locations, and the sharing of that locational data with third parties, creating the potential for panoptical surveillance and a reengineering of reality that carries ontological consequences.

The contextual nature of privacy reinforces an understanding that disclosure contexts and intended audiences are meaningful and relevant. Traditional mechanisms for privacy regulation are challenged by the characteristics of social media, as disclosure is more permanent, sharable and searchable. As these technologies become more ubiquitous and approach near-invisibility in everyday life, understanding the tension between their use and privacy regulation processes becomes more critical. Our third presenter will explore how the utility of social media forms relates to privacy enactment by examining the perceived privacy/sociability trade off. By examining the intersection of sociability and privacy practices among social media users at varying ages we are provided insight into how the utility of these media challenges the conception and understanding of privacy in everyday life.

Finally, our fourth presenter will examine the complicated relationship between anonymity and privacy by undertaking a legal and policy analysis of 'doxxing,' or public shaming. Recently, in response to online sexist and misogynist speech acts, there has been a series of compromises to online anonymity intended to make an offending individual accountable for their actions. But while public shaming may seem to be an effective solution to those who engage in sexist or racist speech acts, it can just as easily be used to further hateful attitudes towards marginalized groups. This presentation will demonstrate how regulating hate speech may not only hold the possibility for negative consequences for online privacy, but also for desired speech such as activism and protest.

By examining privacy and privacy goals through the complex and varied perspectives of technological contexts, practices, and policies, this panel attempts to contribute to our understandings of how privacy is enacted, understood and potentially appropriated in everyday contexts. In doing so, we hope to enhance and refine our understanding of privacy as a desirable and valued outcome.

Keywords

privacy, surveillance, social media, policy, sociability

License

Human Flesh Search Engine: A Discourse of Information Privacy

Jan Fernback
Temple University
USA
fernback@temple.edu

Undrah Baasanjav
Temple University
USA
undrah@temple.edu

Abstract

This study compares U.S. and Chinese news discourses surrounding information privacy policies in relation to the human flesh search engine phenomenon using articles in major print media outlets. Human flesh search engines are a form of crowd sourcing in which thousands of internet users research a phenomenon through social media. Despite its benefits in coordinating resources during the 2008 Chinese earthquakes, HFSE has become controversial due to perceived violations of privacy by the crowd. Using critical discourse analysis, the study finds that international news coverage of HFSE characterizes it as a form of state sponsored vigilantism whereby individual privacy is not only violated, it is all but ignored. Implications focus on the reproduction of Chinese collectivist ideology and the lack of regulation surrounding information privacy**.**

Keywords
privacy; China; social media; critical discourse

Background: Human Flesh Search, Ideology, and Privacy

This work addresses the conference theme through an examination of the reconfiguration of socio-legal-technical practices occurring in the midst of ideological transformations in China. The paper explores the culturally fluid notions of information privacy in connection with the “Human Flesh Search Engine” phenomenon. HFSE is a form of crowd sourcing in which thousands of Internet users research a phenomenon through social media (Chen & Sharma, 2011; Cheong & Gong, 2010; Herold 2011; Wang et al., 2009). It is characterized by both the offline involvement and voluntary activism of internet users, and has also been used to identify people in videos or in photos (Wang, et al., 2010). Chinese social networking sites such as Mop.com, xitek.com, tianya.cn, and sina.com.cn have become collaborative arenas for thousands who search for and share information. However, legal scholars have begun to address information privacy implications surrounding HFS within the context of a transforming political system with emerging privacy law structures.

The consolidation of power by the state in authoritarian regimes takes a new turn with possibilities enabled by the Internet (Mansell, 2004; Morozov, 2011). As an example, the Chinese government has been crowdsourcing censorship by paying netizens to post pro-government comments online and to report on antisocial web cites through HFS (Morozov, 2011). These practices have resulted in a form of *offline* vigilantism that subjects the citizenry to exposure of personally identifiable information and raises privacy concerns. Consequences of exposure via HFS have included public shaming, loss of employment, and forced relocation (Ong, 2012). These questions of human dignity illustrate the tension between privacy rights and rights to free expression. In the United States, these rights are ideally balanced in court cases, however, Chinese privacy law is underdeveloped and linked, ideologically, to traditional collective values.

Privacy Law and Policy and Method

Although privacy is a human right according to the United Nations’ *Universal Declaration of Human Rights* (1948), personal information protection in China is generally not legislated within the context of personal privacy. Chinese communal culture attaches a pejorative connotation to the concept of privacy as something self-absorbed or illegitimate (Maisog, 2009; Wang, 2011). Indeed, the Chinese “culture of shame” elucidated by Confucius has found its way into the General Principles of Civil Law as a means for connecting human dignity, privacy, and reputation. Chinese courts have linked privacy breaches to defamation law since such breaches damage an individual's reputation – a potentially shameful consequence in a communal culture (Ong, 2012). As in U.S. law, Chinese privacy rights conflict with rights to free expression (Wang, 2011). In ancient Chinese culture, the concept of privacy attached to social interests or governmental authority as opposed to individual rights, and civil disputes were generally handled in secret (Wang, 2011). Nevertheless, the concept of privacy developed as an outgrowth of Confucian moralism, similar to the Western notion of natural law (Wang, 2011). With the expansion of economic and technological markets in China and the attendant economic prosperity, the pursuit of individual wealth is more acceptable in Chinese culture. With that pursuit comes an interest in individual rights, particularly as Chinese citizens become exposed to Western values regarding individual freedom. The phrase "this is my privacy" characterizes desires by contemporary Chinese citizens to deflect intrusions into personal matters (Lü, 2005; Wang, 2011).

Critical discourse analysis (CDA) is used in this research to explore news discourses on human flesh search as they relate to privacy and surveillance in the U.S. and China. Discourse analysis is used to clarify the presumable connections between texts, discursive tactics, and sociocultural realities (Fairclough, 1995) with regard to nascent privacy law, the HFS phenomenon, and Chinese political ideology. Specifically, the study addresses how HFS is characterized in terms of information privacy in major news outlets and the ideological, legal, and cultural contexts that may clarify these characterizations.

The study analyzed total of 23 news articles coming from *China Daily* and *The International Herald Tribune (TIHT)*. *China Daily* is the most prominent English-language national daily newspaper on Chinese society, and *TIHT*, the global edition of *the New York Times*, contains extensive international news reporting.

Discussion and Conclusion

Three themes became apparent in the analysis: 1) HFS and individual rights, 2) the power of the crowd and 3) transparency. These themes illustrate an ideological bent in Chinese press coverage of HFS that upholds traditional cultural values regarding shame and privacy couched within an apparent embrace of Western notions of free expression and individual rights. The limited mediated discourse on information privacy in a legal or cultural context reflects both the indeterminate and inchoate nature of privacy law in rapidly changing China. Current Chinese data privacy law does not specify limits upon private information disclosure by non-governmental groups. Nor does it consider the immediate, viral and irremovable nature of information online.

China Daily coverage of HFS shows that Chinese courts neither address privacy concerns nor delineate circumstances under which the right to privacy and the right to reputation are protected. Thus, Chinese legal claimants rarely seek remedies for privacy violation; instead they sue for damage to reputation. *China Daily* discourse indicates how power is co-produced by an elite who maintains the status quo by means including the crowdsourcing of censorship and dismissing local level government officials, and through netizens, who act in the government interest and denigrate others for various reasons of nationalism, financial benefits or simply entertainment. Without well developed privacy laws, the state can easily advance positions against information privacy within a legal framework as an individual right and within an ethical framework as an aspect of human dignity.

Through its discourse of transparency, *TIHT* associates the HFSE phenomenon with the "tyranny of the masses" rather than a potential issue of privacy law. The suffusion of China's historical past into HFS reports suggests an ideology that continues to associate privacy with self-absorption and shame. Thus, newer conceptualizations of privacy that link it to dignity and human rights can be shunted aside, and public discourse about HFS, and concomitantly internet freedom, continues to be coupled with salacious human behavior (shaming, ostracization) and government manipulation of netizens.

Overall, news discourses of privacy surrounding HFS do not reflect new developments in Chinese law that define information privacy and seek some basic protections. Perhaps more importantly, these news discourses center on vigilantism, salaciousness, and so-called free expression. The safeguarding of individual rights is a secondary discourse in the coverage of HFS, but privacy rights have not been characterized as an element within the sphere of state power.

References

Chen, R. & Sharma, S. K. (2011). Human flesh search - Facts and issues. *Journal of Information Privacy & Security, 7*(1), 50-72.

Cheong, P.H. & Gong, J. (2010). Cyber vigilantism, transmedia collective intelligence, and civic participation. *Chinese Journal of Communication, 3*(4), 471-487.

Cho, H., Rivera-Sánchez, M. & Lim, S.S. (2009). A multinational study on online privacy: global concerns and local responses. *New Media and Society, 11* (3). 395–416. DOI: 10.1177/1461444808101618

Cohen, J. (2012). *Configuring the networked self: Law, code, and the play of everyday practice.* New Haven: Yale University.

Fairclough, N. (1995). *Media discourse*. London: Edward Arnold.

Herold, D. K. (2011). Human flesh search engine: Carnivalesque riots as components of a "Chinese Democracy." In D. K. Herold & P. Marolt (Eds.), *Online society in China: Creating, celebrating, and instrumentalising the online carnival* (pp. 127-145). Abingdon, Oxon: Routledge.

Lü, Y. H. (2005). Privacy and data privacy issues in contemporary China. *Ethics and Information Technology 7,* 7–15. DOI 10.1007/s10676-005-0456-y

Maisog, M.E. (2009). *Personal Information Protection in China.* Beijing, China: Hunton & Williams LLP. Retrieved Jan 15, 2013 from http://www.huntonfiles.com/files/webupload/PrivacyLaw_Personal_Information_Protection_in_China.pdf

Mansell, R. (2004). Political economy, power and new media. *New Media and Society,* 6 (1). 96–105.

Morozov, E. (2011). *The net delusion: The dark side of Internet freedom.* NYC: Public Affairs.

Ong, R. (2012). Online vigilante justice Chinese style and privacy in China. *Information & Communications Technology Law, 21*(2), 127-145. DOI: http://dx.doi.org/10.1080/13600834.2012.678653

United Nations. (1948). *Universal Declaration of Human Rights.* Retrieved Jan 28, 2013 from http://www.un.org/en/documents/udhr/index.shtml

Wang, B., Hou, B. Yao, Y. & Laibin, Y. (2009). Human flesh search model: Incorporating network expansion and gossip with feedback. *Proceedings of the Distributed Simulation and Real Time Applications.* Singapore, 82-88. DOI:10.1109/DS-RT.2009.36

Wang, F.Y., Zeng, D., Hendler, J. A., Zhang, Q., Feng Z., Gao, Y. , Wang, H. & Lai, G. (2010). A study of the human flesh search engine: Crowd-powered expansion of online knowledge. *Computer (IEEE Computer Society), 43*(8), 45-53. doi:10.1109/MC.2010.216

Wang, H. (2011). *Protecting privacy in China*. Berlin: Springer-Verlag.

Privacy and Augmented Mobility

Michael Zimmer
University of Wisconsin – Milwaukee
USA
zimmerm@uwm.edu

Abstract

The emergence of augmented mobility technologies brings forth profound transformations and challenging problems for our contemporary information society, particularly regarding privacy and surveillance. Location-aware mobile Internet applications provide new layers of information to aid in navigation, decision-making, and social interactions. But they also require widespread tracking, collecting, and aggregating of users' precise locations, and the sharing of that locational data with third parties, creating the potential for panoptical surveillance. And while augmented reality mobile applications help us, for example, recognize places and faces, and interact with our physical world armed with layers of information not otherwise accessible, they also can lead to privacy-invading facial recognition tools, and give content providers new ability to regulate and rationalize how we understand our world through the control of the information layers presented. This paper will introduce emerging infrastructures of augmented mobility technologies, and critically interrogate their impact on conceptions – and expectations – of privacy in our infosphere.

Keywords

privacy; augmented mobility; augmented reality; surveillance; ethics

Augmented Mobility

We increasingly are living in what the information philosopher Luciano Floridi (2007) describes as an "infosphere." A neologism of "information" and "biosphere," Floridi's concept of the infosphere denotes our whole informational environment. More than just an "information society" or even the set of networked domains commonly referred to as "cyberspace," the infosphere is an environment that includes *all* information spaces and interactions, online and off, digital and analog. Conceptualizing our surroundings as an infosphere recognizes how information is increasingly enveloping our environment – information is *becoming* our ecosystem – and where, as Floridi puts it, "the threshold between *here* (*analog, carbon- based, offline*) and *there* (*digital, silicon-based, online*) is fast becoming blurred" (p. 61).

This blurring is perhaps most visible when we consider the recent emergence of advanced mobile technological infrastructures providing new information layers in multiple domains of everyday life. These include three categories of particularly innovative technological platforms: *location-aware mobile Internet applications*, *augmented-reality mobile applications*, and the convergence of these within *wearable augmented reality devices*.

Location-aware mobile Internet applications represent a growing set of mobile software tools developed for handheld devices such as personal digital assistants, tablet computers, and smartphones, that deliver new layers of information to users in real-time based on their physical location. Application developers employ GPS, cellphone infrastructures, or wireless access points to identify where devices are located, and users can choose to share that information with location-aware applications. Those applications can then provide users with resources such as a "you are here" marker on a city map, reviews for restaurants in the area (Yelp), a nap alarm that's triggered by your specific stop on a commuter train, or notices about nearby bottlenecks in traffic. Applications might also report a user's location to friends in a social network, prompting those nearby to meet for coffee or dinner, or simply provide relevant advertising based on a user's present geographic location. This growing category of mobile Internet applications provides enhanced environmental awareness, offering users a location-based layer of information to guide their daily activities and interactions.

Augmented-reality mobile applications integrate layers of digital information or imagery within a live, real-world physical encounter typically viewed from a smartphone camera and display (Parr, 2009). While location-aware applications provide layers of geographic information on artificial displays, augmented-reality layers informational objects onto a physical environment in real-time, allowing users to see supplementary information to aid their perception of the real world and to interact with it. Examples include Layar, which overlays information from Wikipedia, Yelp, and other sources on top of live camera images of your current location, Augmented ID, which identifies a person’s face and overlays her social networking profile information on a smartphone’s display while looking at the individual, and augmented driving applications that provide real-time detection and identification of vehicles and obstacles to assist with driving and vehicle safety. The combination of large-display smartphones and high-speed mobile Internet service continue to push the development of these highly innovative and helpful applications.

Wearable augmented reality devices represent the latest technological evolution of augmented mobility, where the user interface and display of new informational layers becomes more integrated with the user. While the augmented-mobility applications described above typically rely on the presence of a smartphone or similar external device held by a user, wearable augmented reality devices bring the technology one step closer to the body, provide a more transparent and effortless interface for providing real-time layers of information to users.

In early versions, augmented reality technology involved specialized equipment such as goggles or head-mounted displays, and depended on bulky computers tethered to or carried by users. Miniaturization of processors, sensors, and battery technologies has helped refine these systems and make them more consumer-friendly, such as the Vuzix Wrap 920AR augmented reality glasses (Webb, 2010) which provide rudimentary 3D imaging through (still somewhat bulky) glasses-mounted stereoscopic cameras that can seamlessly blend computer-generated imagery with what the user “sees.”

More advanced prototypes show the great potential of wearable augmented reality devices. Examples include the (still experimental) SixthSense gestural interface, which projects an information layer onto objects the user interacts with without need of special glasses or displays (Pogue, 2009), and the much-anticipated “Glass Project” from Google, which has the potential to augment information-seeking, navigation, and personal interaction through voice-controls and displaying layers of information to users in an unobtrusive heads up display on a small eyeglass frame (Gannes, 2012).

Taken together, *location-aware mobile Internet applications* and *augmented reality mobile applications*, and *wearable augmented mobility devices* strive to provide new information layers for our mobile lives, promising to deliver information not otherwise accessible, combining real and informational objects interactively and seamlessly to provide augmented means of exploration, learning, and social interaction. Their continued development and deployment are fostering the emergence of new *augmented mobility platforms*, which increasingly define our infosphere and how we exist within it.

Privacy and Augmented Mobility

When Floridi (2007) ponders the impact of new information technologies and infrastructures on our infosphere, he speaks of the “reontologization of our environment and of ourselves” (p. 62). This reontologizing refers to a very radical form of reengineering, one that not only designs, constructs, or structures a system anew, but that fundamentally transforms its intrinsic nature. Reontologizing is about the ontological consequences of the reengineering of reality that happens through converging technologies.

Emerging augmented mobility platforms are information-rich, constant, and all-encompassing technologies that promise to provide new ways of conceiving of our world: locational information presents new layers of meaning and possibilities of action; augmented realities provide entirely new interfaces and means of interacting with our environments; wearable devices remove the sense of mediation and present informational layers as an increasing natural part of our environment. In this sense, augmented mobility technologies are not merely providing new information layers – not merely reengineering how we interface with our reality – but actually reontologizing our environment, our infosphere. As Floridi {%Floridi, 2007, #4655} explains:

> The infosphere will not be a virtual environment supported by a genuinely "material" world behind; rather, it will be the world itself that will be increasingly interpreted and understood informationally, as part of the infosphere. (p. 61)

The consequences of this reontologization of our infosphere by augmented mobility technologies are both positive and negative, enhancing and threatening. In his writing about "everyware," a paradigmatic conception of the emergence of ubiquitous and pervasive computing, Adam Greenfield (2006) warns of the duplicitous effects of these emergent technologies. On the one hand,

> The appeal of all this is easy to understand. Who wouldn't desire a technology that promised to smooth the edges of modern life, subtly intervene on our behalf to guide us when we're lost, and remind us of the things we've forgotten? …The vision is a lovely one: deeply human, even compassionate. (p. 2)

But at the same time, Greenfield warns,

> [We] will have to reckon with the emergent aspects of our encounter with everyware, with all the ways in which its impact turns out to the something unforeseeably more than the sum of its parts. …[E]veryware will surface and make explicit facts about our world that perhaps we would be happier ignoring. In countless ways, it will disturb unwritten agreements about workspace and homespace, and the presentation of self and the right to privacy. It contains an inherent, unsettling potential for panoptical surveillance, regulation, and "rationalization." Its presence in our lives will transfigure our notions of space and time, self and other, citizen and society in ways that we haven't begun to contemplate. (pp. 2-3)

Greenfield's concern over the dual risks and rewards of the ubiquitous computers that make up his "everyware" are equally present when considering the reontologizing effects of ubiquitous mobility technologies in the infosphere. Location-aware mobile Internet applications provide new layers of information to aid in navigation, decision-making, and social interactions. But they also require widespread tracking, collecting, and aggregating of users' precise locations, and the sharing of that locational data with third parties, creating the "unsettling potential for panoptical surveillance" Greenfield warns us of. And augmented reality mobile applications help us, for example, recognize places and faces, and interact with our physical world armed with layers of information not otherwise accessible. But they also can lead to privacy-invading facial recognition tools, and give content providers new ability to regulate and rationalize how we understand our world through the control of the information layers presented.

Following Greenfields concerns, this paper will introduce emerging infrastructures of augmented mobility technologies, and critically interrogate their impact on conceptions – and expectations – of privacy in our infosphere.

References

Floridi, L. (2007). A look into the future impact of ICT on our lives. *The Information Society*, *23*(1), 59–64.

Gannes, L. (2012). Google Unveils Project Glass: Wearable Augmented-Reality Glasses. *AllThingsD*. Retrieved from http://allthingsd.com/20120404/google-unveils-project-glass-wearable-augmented-reality-glasses/

Greenfield, A. (2006). *Everyware: The Dawning Age of Ubiquitous Computing*. Berkeley, CA: New Riders Publishing.

Parr, B. (2009). Top 6 Augmented Reality Mobile Apps. *Mashable.com*. Retrieved from http://mashable.com/2009/08/19/augmented-reality-apps/

Pogue, D. (2009). At TED, Virtual Worlds Collide With Reality. *New York Times* - *Pogue's Posts*. Retrieved from http://pogue.blogs.nytimes.com/2009/02/11/at-ted-virtual-worlds-collide-with-reality/

Webb, M. (2010). Vuzix display Wrap 920AR augmented reality glasses. *gizmag*. Retrieved from http://www.gizmag.com/vuzix-wrap-920ar-augmented-reality-glasses/13847/

License

The Big Share: Reconciling Sociability and Privacy in Social Media Use

Kelly Quinn
University of Illinois at Chicago
USA
kquinn8@uic.edu

Abstract

The contradiction between the stated preferences of social media users toward privacy and actual privacy behaviors has suggested a willingness to trade privacy regulation for social goals. This study employs data from a survey of approximately 350 social media users which collected data on privacy attitudes, online privacy strategies and behaviors, and perceptions of the utility that social media experiences bring. This research enhances the understanding of the contextual dimensions privacy regulation processes by examining how individuals perceive the relationship between sociality and privacy in social media use, how these relate to gratifications derived from social media engagement, and how differences may surface among users at varying points in life. This study lends greater nuance to how the dynamic of privacy and sociality is understood and enacted by users, and how privacy and social goals may intersect at varying points in life.

Keywords

Privacy; sociality; social media; life course;

Background

The use of social media has moved from normal into ubiquitous, with 67% of all US adults using social network sites today and significantly higher levels of use evident among young adults and females (Duggan and Brenner, 2013). Yet these technologies continue to challenge the mechanisms for control and access to private information, as established mechanisms of boundary maintenance in everyday life— discriminatory communication with defined groups of others or selective disclosure of information—are not easily accomplished when using these platforms. As the use of these technologies move toward invisibility because of their mundane nature, it becomes critical to understand how they relate to core values and ideals such as the ability to regulate privacy in everyday life.

Research on internet and social media users has demonstrated that while individuals have strong concerns about their privacy online (Buchanan, Paine and Joinson, 2007; Young and Quan-Hasse, 2009), they do not understand and/or do not engage privacy controls to contain disclosure (Debatin, Lovejoy, Horn and Hughes, 2009; Tufecki, 2008), do not read privacy policies when registering on a website (Milne & Culnan, 2004), and disclose sensitive information (Strater and Lipford, 2008). There is often a mismatch between users' stated preferences and actual behaviors, as online actions and disclosures do not correspond to users level of apprehension regarding privacy (Acquisti and Gross, 2006; Ahern, et al., 2007; Debatin, et al., 2009; Fogel and Nehmad, 2008; Tufecki, 2008; Stutzman, Capra and Thompson, 2011). This presents a contradiction between privacy preferences and privacy behaviors that has puzzled researchers.

One perspective on this paradox is that realization of the social capital benefits of participation in social network sites requires a perceived need to exchange personal information (Ellison, Vitak, Steinfeld, Gray and Lampe, 2011). Others indicate that the risk of disclosure is mitigated by the convenience that social network sites offer for relational management (Krasnova, Spiekermann, Koroleva and Hildebrand, 2010). While this research is an important step in understanding the trade-offs users make between privacy regulation and social goals, these studies have concentrated on populations of young adult social media users.

Younger adults use the internet for building and maintaining interpersonal relationships more than midlife and older adults (Thayer and Ray, 2006; Zickuhr and Madden, 2012) and younger and older users experience different motivations and usage patterns when using social media (Brandtzæg, Lüders, and Skjetne, 2010), so a focus on how young adults view the tension between privacy regulation and sociality may diminish cultural and cohort differences embedded within relational practices and the differing values that arise among users of varying backgrounds and life experiences. More work is required to understand how the dialectic of privacy regulation and sociality is understood and enacted by a wider range of users, and how it might vary at different points in the life course.

This study attempts to provide texture to the understanding of the contextual dimensions of informational privacy regulation by examining how individuals perceive the relationship between sociality and privacy in their social media use, and how these relate to the gratifications derived from engagement. Of particular interest is examination of how the intersection of behaviors, attitudes and utility derived from social media use might vary at different points in the life course.

Literature

Online informational privacy regulation is a complex process, involving control of the release of personal information to others (Altman, 1975), an expectation of the intended audience (Brake, 2012; Nippert-Eng, 2010), and the context in which disclosure takes place (Nissenbaum, 2010); however from a research perspective, privacy regulation has been approached as a unidimensional construct (Buchanan, et al, 2007), captured by activation of technological privacy controls (Stutzman and Kramer-Duffield, 2010), the presence of personally identifying information on SNS profiles (Acquisti and Gross, 2006), or the visibility of profile information (Thelwall, 2009). Privacy settings, connection decisions and the extent of information disclosure are all components of privacy regulation on social network sites (Ellison, et al., 2011; Krasnova et al., 2010). Without evaluating these multiple levels of context and disclosure, or considering the related gratifications of social media use, little guidance can be provided for privacy-enhancing design improvements for these technologies.

Method

Approximately 350 social media using adults are targeted to participate in a self-administered, web-based survey designed to collect data related to privacy attitudes, online privacy strategies and behaviors, and perceptions of the utility and satisfaction that social media experiences bring. The sampling strategies are designed to recruit participants varying in age so that statistical comparisons might be made among social media users at varying points in life.

Implications

Prior research has indicated that the utility of social media may shift downward as one ages (Brandtzæg, et al., 2010); this may be reflective of lower overall participation rates in social media (Zickuhr and Madden, 2012), making communication with one's social network via social media a less effective tool, or possibly that social media is perceived as having reduced salience for sociality as one ages (Lehtinen, Näsänen, and Sarvas, 2009). Because the utility of social media has been indicated to be of significance in privacy regulation processes for younger adults (Ellison, et al., 2011; Krasnova et al., 2010), examining its relationship to privacy attitudes and behaviors at differing points in life will provide a more nuanced perspective on how the dynamic of privacy and sociality is understood by users. Examination of this dialectic at varying points in life will also lend insight into how the contextual dimensions of privacy regulation intersect with social media use and are enacted in the everyday. As these media forms move toward near invisibility, understanding this dynamic becomes imperative, not only because insight into privacy regulation processes will point to ways in which system design might be improved to provide meaningful privacy enhancements, but also because it enables a greater appreciation of how these media forms shape core values and ideals.

References

References are APA Style and Times New Roman 10, Aligned Left, Single Line, 0pt before, 6pt after, hanging 0.5 inches).

Acquisti, A. & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy Enhancing Technologies* (pp. 36-58). Cambridge, UK: Springer-Verlag.

Ahern, S., Eckles, D., Good, N. S., King, S., Naaman, M. & Nair, R. (2007). Over-exposed? Privacy patterns and considerations in online and mobile photo sharing. In *Proceedings of the SIGCHI conference on human factors in computing systems - CHI '07* (p. 357). New York, New York, USA: ACM Press. doi:10.1145/1240624.1240683

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Publishing.

Brake, D. R. (2012). Who do they think they're talking to? Framings of the audience by social media users. *International Journal of Communication*, *6,* 1056–1076. Retrieved from http://ijoc.org/ojs/index.php/ijoc/article/view/932/747

Brandtzæg, P. B., Lüders, M. & Skjetne, J. H. (2010). Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *International Journal of Human-Computer Interaction*, *26*(11-12), 1006–1030. doi:10.1080/10447318.2010.516719

Buchanan, T., Paine, C. B., Joinson, A. N. & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science, 58*(2), 157–165. doi:10.1002/asi

Debatin, B., Lovejoy, J. P., Horn, A.-K. & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108. doi:10.1111/j.1083-6101.2009.01494.x

Duggan, M. & Brenner, J. (2013, 14 Feb). *The Demographics of SocialMedia Users — 2012.* Washington, DC: Pew Internet & American Life Project. Retrieved from http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R. & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.*), Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 19-32). Berlin: Springer Berlin Heidelberg. doi:10.1007/978-3-642-21521-6

Fogel, J. & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160. doi:10.116/j.chb.2008.08.006

Krasnova, H., Spiekermann, S., Koroleva, K. & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109-125. doi:10.1057/jit.2010.6

Lehtinen, V., Näsänen, J., & Sarvas, R. (2009). " A Little Silly and Empty-Headed " – Older Adults ' Understandings of Social Networking Sites. *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology - BCS-HCI '09* (pp. 45–54). Swinton, UK: British Computer Society.

Milne, G. R. & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15-29. Elsevier. doi:10.1002/dir.20009

Nippert-Eng, C. (2010). *Islands of Privacy*. Chicago: University of Chicago Press.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy and the Integrity of Social Life.* Stanford, CA: Stanford Law Books.

Raynes–Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1), 1–8. Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432

Strater, K. & Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. In D. England (Ed.), *BCS-HCI '08 Proceedings of the 22nd British HCI Group Annual*

Conference on People and Computers: Culture, Creativity, Interaction - Volume 1 (pp. 111-119). Swinton, UK: British Computer Society.

Stutzman, F., Capra, R. & Thompson, J. (2010). Factors mediating disclosure in social network sites. *Computers in Human Behavior, 27*(1), 590-598. doi:10.1016/j.chb.2010.10.017

Thayer, S. E. & Ray, S. (2006). Online communication preferences across age, gender, and duration of Internet use. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society, 9*(4), 432–440. doi:10.1089/cpb.2006.9.432

Thelwall, M. (2009). Social network sites: users and uses. In M. Zelkowitz (Ed.), *Advances in computers: Social networking and the web,* Vol. 76, *(*pp. 19–73). Elsevier: Amsterdam.

Tufekci, Z. (2007). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20-36. doi:10.1177/0270467607311484

Young, A. L. & Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites. *Proceedings of the fourth international conference on Communities and technologies - C&T '09* (p. 265). New York: ACM Press. doi:10.1145/1556460.1556499

Zickuhr, K. & Madden, M. (2012). *Older adults and internet use,* Pew Internet & American Life Project, Washington, DC. Retrieved from http://pewinternet.org/Reports/2012/Older-adults-and-internet-use.aspx Consalvo, M. (2006). Console video games and global corporations: creating a hybrid culture. *New Media & Society 8* (1), 117-213. doi: 10.1177/1461444806059921.

License

There's No Justice Like Angry Mob Justice:

Regulating Hate Speech through Internet Vigilantism

Alice Marwick
Fordham University
USA
amarwick@fordham.edu

Abstract

This paper undertakes a legal and policy analysis of public shaming, or "doxxing," as a possible solution to sexist and misogynist online speech acts. First, government and private regulation of certain types of internet speech are evaluated, concluding that neither is a viable solution. Second, incidents in which internet vigilantism has been used to both regulate and further internet hate speech are discussed. Third, privacy issues around vigilantism, which often involves revealing secret or obscure information, are analyzed. While doxxing may seem to be a useful tool for regulation, it is as frequently used to further online sexism as to prevent it. However, alternatives for regulating hate speech have possibly unforeseen negative repercussions for online privacy, including the maintenance of anonymity.

Keywords

Hate speech; free speech; sexism; misogyny; internet policy

Introduction

While gender equality in the United States made significant gains from the 1950s to the 1990s, research has found a recent slowdown in such attitudes (Cotter, Hermsen, & Vanneman, 2011). Scholars have documented repeated instances of aggressively sexist and misogynistic internet speech of late, often including harassment of individual women (Bartow, 2009; Citron, in press). The possible effects of such acts include a chilling effect on women's online participation; long-term emotional and professional difficulty for the women harassed; and an increase in sexual stereotyping and discrimination off and online (Nussbaum, 2010).

The best way to deal with such speech acts, as well as similar speech involving racist and/or homophobic language, is an ongoing question. US government regulation is unlikely given the Supreme Court's consistent characterization of internet speech as protected. There are at least two alternative mechanisms for regulation. The first involves private corporations such as Facebook defining certain categories of speech as unacceptable in their Terms of Service, allowing for individual accounts which violate these terms to be removed. The second involves public unmasking of anonymous or pseudonymous accounts, known colloquially as "doxxing" or "internet vigilantism." Underlying doxxing is the belief that individuals are unlikely to undertake hateful speech acts under their own names, as this may result in social ostracizing, job loss, and so forth.

This paper undertakes a legal and policy analysis of the privacy issues inherent in the latter means of regulation. Doxxing may seem to be a useful regulatory mechanism, but it is as frequently used to further online sexism as it is to prevent it. However, alternatives for controlling hateful speech have potential privacy implications, including compromising anonymity.

Background

In the last decade, several high-profile incidents have raised questions around the limits of online free speech and the prevalence of explicitly sexist commentary on the internet (Citron, 2009). As a result, some scholars have called for regulation of online "hate speech" or online defamation (Levmore, 2010).

The United States Supreme Court has consistently held up Internet speech as entitled to the same protections as print and spoken speech, most notably in *Reno vs. ACLU*. This is unique to the United States as other localities have consistently regulated online speech (Vanacker, 2006). Given the lack of government regulation, organizations have turned to the private sector. For example, groups like the Anti-Defamation League and the Southern Poverty Law Center have pressured ISPs into refusing to host hate sites (Henry, 2009). Ultimately, the ambiguity of "hate speech" as a category, the lack of resources for moderation relative to the amount of content created on social media sites, and the "Safe Harbor" provision of the Digital Millennium Copyright Act, make it unlikely that the private sector will proactively moderate specific types of speech acts.

Internet Vigilantism and Doxxing

The internet has seen a recent swath of public shaming and unmasking of individuals for engaging in particular speech acts. Violentacrez, a popular Reddit user who maintained communities promoting candid photography of underage girls, had his "real" identity revealed by Gawker. The feminist blog Jezebel publicized the Twitter names and avatars of teenagers who used racial epithets to refer to President Obama. Previously, internet vigilantism was rarely targeted towards people engaging in hateful speech; rather, it was used to punish people who violated social norms, such as the "Dog Poop Girl" in South Korea who let her dog defecate in a subway car (Wehmhoener, 2010).

In fact, internet vigilantism has been more frequently used to further misogyny rather than counter it. A prominent example is Anita Sarkeesian's Feminist Frequency project. Sarkeesian, a feminist filmmaker and cultural critic, proposed a series of "Tropes vs. Women" videos focusing on images of women in video games. She was subsequently attacked by anonymous individuals who sent her pornographic images, left thousands of comments containing sexual and misogynistic epithets, and created a web-based game that allowed players to "Beat Up Anita Sarkeesian" (O'Leary, 2012).

Privacy Issues

Doxxing and public shaming often involve the reveal of personal information. In some cases, a carefully protected persistent pseudonym is linked to an "offline" identity. In others, an anonymous citizen is identified using digital technologies, such as crowdsourcing the identity of a photographed street vandal. Sometimes, an anonymously-posted piece of internet content, such as a YouTube video, is associated with an IP address or physical location. These cases share an underlying presumption that by revealing personally identifiable information, an anonymous individual will be brought into the public eye and be made accountable for their actions. This "shame justice" is not motivated by rehabilitation but to punish the offender as drastically as possible (Parsons, 2012).

In the famous AutoAdmit case, commenters on a law school message board posted hundreds of violent and sexual comments about female law students. These comments were searchable and appeared as search engine results for the female students' names, harming their reputation. Nussbaum argues that this attempt was motivated by a desire to shame the law students for their success in a male-dominated world. Thus, shame is utilized both by feminists—when attempting to unmask sexist commenters—and misogynists alike. In most of these cases, the doxxers or vigilantes remain anonymous, while the target is shamed as publically as possible.

Critics of internet hate speech call for eliminating online anonymity, with the proposed consequence of eliminating unwanted online speech acts (Levmore, 2010). However, anonymity has a complicated relationship to privacy. On one hand, anonymity can be necessary for the free expression of speech, most obviously for people like political activists with a heightened need for safety. On the other hand, anonymity allows for hateful comments to be made without reprecussion. If internet vigilantism is positioned as the logical alternative to the lack of government or private regulation of online speech, it may compromise anonymity, which is a necessary aspect of free speech.

Conclusion

There is no clear or easy answer to the problem of sexist, racist, or homophobic commentary online. Even characterizing this speech as “hate speech” sets up a particular category of speech as less protected, which has not held up under strict scrutiny in the US courts. While public shaming may seem to be an effective solution to those who engage in sexist or racist speech acts, it can just as easily be used to further hateful attitudes towards marginalized groups. Ultimately, each of the current alternatives for regulating hate speech have possibly unforeseen negative repercussions not only for online privacy, but for desired speech such as activism and protest.

References

Bartow, A. (2009). Internet Defamation as Profit Center: The Monetization of Online Harassment. *Harvard Journal of Law and Gender*, *32*(2). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1447472

Citron, D. (in press). *Hate 3.0.* Harvard University Press.

Citron, D. (2009). Cyber Civil Rights. *Boston University Law Review*, *89*, 61–125.

Cotter, D., Hermsen, J. M., & Vanneman, R. (2011). The End of the Gender Revolution? Gender Role Attitudes from 1977 to 20081. *American Journal of Sociology*, *117*(1), 259–289.

Henry, J. S. (2009). Beyond free speech: novel approaches to hate on the Internet in the United States. *Information & Communications Technology Law*, *18*(2), 235–251.

Levmore, S. (2010). The Internet’s Anonymity Problem. In S. Levmore & M. C. Nussbaum (Eds.), *The Offensive Internet* (pp. 50–67). Cambridge, MA: Harvard University Press.

Nussbaum, M. C. (2010). Objectification and Internet Misogyny. In S. Levmore & M. C. Nussbaum (Eds.), *The Offensive Internet* (pp. 68–87). Cambridge, MA: Harvard University Press.

O’Leary, A. (2012, August 1). Sexual Harassment in Online Gaming Stirs Anger. *The New York Times*. Retrieved from http://www.nytimes.com/2012/08/02/us/sexual-harassment-in-online-gaming-stirs-anger.html

Parsons, C. (2012). *Shame Justice on Social Media: How it Hurts and Ways to Limit it* (SSRN Scholarly Paper No. ID 2151204). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=2151204

Vanacker, B. H. (2006). *Online Hate Speech Regulation in the United States and Europe: Accommodating Conflicting Legal Paradigms* (Doctoral Dissertation). University of Minnesota, Minneapolis.

Wehmhoener, K. A. (2010). Social norm or social harm: An exploratory study of Internet vigilantism. Retrieved from http://lib.dr.iastate.edu/etd/11572/