Information and Consent

Amy Adele Hasinoff
University of Colorado Denver
USA
amy.hasinoff@gmail.com

Abstract

In 1999, a technology CEO stated: "You have zero privacy. Get over it." Is it true that privacy is impossible online? By socializing on the internet and on mobile devices, users deliberately and inadvertently generate personal artifacts and data. While people have significant interests in protecting their private personal information online, the existing rhetorical and legal tools to do so are limited. The solution proposed here is to adopt a standard that explicit consent should be necessary for the production, distribution, or possession of private media content and information. Given the quantity of personal information created and stored in digital formats, scholars, policymakers, technology developers, and users alike need to develop social norms and technological mechanisms for obtaining meaningful and informed consent before circulating private information.

Keywords

consent; privacy; sexting; sexuality

Introduction

There an interesting contradiction in how we think about the capacity and right to control information. On one hand, there is broad legal and public support for the control of commercially produced information and media. From intellectual property and patent laws to copyright infringement lawsuits, the law and the public seem to generally support companies' rights to own and control the information and media content they create. At the same time, users are told that "information wants to be free," "privacy is dead," and that giving up control over their information and personal content is necessary for the success and progress of the information economy. The public benefit of unrestricted information flows has been ceaselessly promoted without careful consideration of who and what suffers. Most forms of data mining are legal, governments engage in sophisticated surveillance programs, and public records that were once difficult to access are now freely available online. The common idea that personal information is impossible to control is particularly problematic when it allows legal and educational authorities to punish teens who create sexual images of themselves while completely ignoring malicious forwarders (Hasinoff, forthcoming).

By using the internet and mobile devices, people deliberately and inadvertently generate personal artifacts and data that can be persistent, easily replicable, and even searchable (boyd, 2008). Given the quantity of personal information created and stored in digital formats, and the privacy concerns related to the technological ease of its circulation, scholars, policymakers, technology developers, and users alike need to think more seriously about consent in digital media. As Nissenbaum (2011) points out, it is vital to find ways to adapt existing offline norms for privacy for online contexts. While most people have significant interests in protecting their private personal information against commercial exploitation, the existing rhetorical and legal tools to do so are limited. While copyright and crime prevention are often seen as legitimate reasons to restrict the flow of information, others, such as privacy and cultural preservation, are weakly and inconsistently protected (Nissenbaum, 1998; Seeger, 2005; Solove, 2007; Weintraub & Yung, 2009).

An Explicit Consent Standard

The solution proposed here is to adopt a standard that explicit consent should be necessary for the production, distribution, or possession of private media content and information. This can help address

the complexities of privacy in digital media and challenge the idea that information should always be free. This new norm asks people to actively seek consent if they want to distribute another person's private media or information. This has a range of implications, from suggesting that one should always ask for permission before distributing a private photo of someone else, to requiring that websites that aggregate and re-sell personal information should obtain informed and meaningful consent from users. There are legal changes that could come out of the explicit consent model, but the idea of building consent into models of private media circulation is most powerful as a new social norm that can help transfer existing ideas about offline privacy to an online context.

This explicit consent model is built on the feminist debates about sexual consent in the late 1980s and early 1990s. In response to the social and legal failures to adequately address non-stranger sexual violence, these feminist reformers advocated changing the way people think about sexual consent. Scholars including Estrich (1987), Pineau (1989), and Remick (1993) argue that assumptions and nonverbal cues are insufficient to determine consent in sexual activity. They point out that prosecutors working with conventional understandings of rape must prove that the complainant resisted; in some states this resistance must still be physical, while in others the victim is required to have verbally resisted (Little, 2005). In contrast, according to the affirmative consent model, rape is defined by the absence of a clear and voluntary "yes." That is, these reformers argue that the default assumption should be "no," and the sexual initiator should always obtain clearly articulated and freely given consent. As Kasubhai (1997) points out, there are already strict standards of informed, voluntary consent in non-sexual situations of potential personal intrusion, such as medical procedures and warrantless searches, in which neither silence nor agreeing under duress constitute valid consent.

There are already many privacy norms for offline social interactions that can provide a meaningful guide for how to interpret what content should be considered private. Nissenbaum (2011) argues that privacy is indeed possible online by pointing out that the internet is best conceived as a new place to enact a variety of mostly pre-existing social and commercial relations, from banking and shopping to conducting research and chatting with friends. For example, a commercially produced sexual image is not intended to be private; thus a person buying pornography would not need to obtain consent. However, since people usually view their sexual acts as private, they can likely also recognize that others' personal sexual images will be typically private as well. While further study of the expectations of privacy and understandings of consent in digital media is necessary, Albury and Crawford (2012) argue that young people are already developing norms and ethics of sexting that respect privacy and consent. Consider that before the internet and mobile phones, people created and selectively shared personal sexually explicit letters and photos, using a polaroid camera, for example, and would be able to reasonably expect that person to refrain from showing them to parents, friends, and future employers. Mobile phones make it far easier to violate privacy by digitally forwarding such content, but Nissenbaum's argument stipulates that the old information norms can and should remain when social behaviors become mediated and digitized.

The power of an explicit consent standard is that it clearly establishes that the default is that it is not acceptable to distribute private information. Requiring explicit consent means that the burden to obtain consent is shifted onto the person who wants to produce, distribute, or possess private content. In such cases, some formal or informal agreement or strong precedent would be necessary to establish consent for the circulation of private content or information. Currently, the default settings on social media applications often assume that people want to share all their personal information, which has the greatest impact on the least skilled users (boyd & Hargittai, 2010). Incorporating an explicit consent model at the level of design (Cavoukian, 2009) could better serve users' interests. For example, while mobile phone users can typically forward any image they receive, an explicit consent standard might suggest that this feature should be disabled by default. In this case, the user who creates an image could decide to either keep this privacy restriction or to mark the image as public and thus possible to forward by anyone who receives it. Such user-controlled DRM could help enact consent norms.

Conclusion

It is vital to challenge the assumptions that everything digital is public and everything public can be publicized. People routinely trust their lovers, doctors, and loan officers with personal information that they expect will not be distributed; an explicit consent standard is a way to extend existing privacy norms to digital media. We need logics of information protection and restriction that account for the range of reasons people may have to limit the free flow of their personal information and content, including privacy, cultural preservation, and personal safety. Surrendering all the decisions about the circulation of private information to market forces will not adequately protect our privacy.

Acknowledgments

References

Albury, K., & Crawford, K. (2012). Sexting, consent and young people's ethics: beyond Megan's Story. *Continuum, 26*(3), 463-473.

boyd, d. (2008). Why youth (heart) social network sites: the role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, identity, and digital media* (pp. 119–142). Cambridge, MA: MIT Press.

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8).

Cavoukian, A. (2009). *Privacy by design ... take the challenge*. Available from http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf

Estrich, S. (1987). *Real Rape*. Cambridge, MA: Harvard University Press.

Hasinoff, A. A. (forthcoming). *How to think about sexting*. Champaign, IL: University of Illinois Press.

Kasubhai, M. T. (1997). Destabilizing power in rape: why consent theory in rape law is turned on its head *Wisconsin Women's Law Journal, 11*, 37-74.

Little, N. J. (2005). From no means no to only yes means yes: the rational results of an affirmative consent standard in rape law. *Vanderbilt Law Review, 58*, 1321-1364.

Nissenbaum, H. (1998). Protecting privacy in an information age: the problem of privacy in public. *Law and Philosophy, 17*, 559-596.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Dædalus, the Journal of the American Academy of Arts & Sciences, 140*(4), 32-48.

Pineau, L. (1989). Date rape: a feminist analysis. *Law and Philosophy, 8*, 217-243.

Remick, L. A. (1993). Read her lips: an argument for a verbal consent standard in rape. *University of Pennsylvania Law Review, 141*, 1103-1151.

Seeger, A. (2005). Who got left out of the property grab again? Oral traditions, indigenous rights, and valuable old knowledge. In R. A. Ghosh (Ed.), *CODE: Collaborative ownership and the digital economy* (pp. 75-84). Cambridge, Mass.: MIT Press.

Solove, D. J. (2007). *The future of reputation: gossip, rumor, and privacy on the Internet*. New Haven: Yale University Press.

Weintraub, A. N., & Yung, B. (Eds.) (2009). *Music and Cultural Rights*. Chicago: University of Illinois Press

License