Something to Hide: Individual Strategies for Personal Privacy Practices

Courtney Loder[1]
[1] University of California Irvine

Abstract
This paper illustrates the strategies by which individual users are beginning to take control of their personal data streams, and the way that social practices are developing as a way to overcome longstanding usability hurdles for third party privacy management tools, particularly encryption. Grounded in an historical overview of telecommunications policy in the United States as it relates to the development of computer-mediated communication, contemporary notions of privacy are discussed. Preliminary analysis from pilot interviews and the early development of CryptoParty are presented to illustrate sites where the work of individual privacy regulation occurs, and is taught to others.
Keywords: privacy, encryption, personal data management, information policy
Citation: Loder, C. (2014). Something to Hide: Individual Strategies for Personal Privacy Practices. In *iConference 2014 Proceedings* (p. 814–819). doi:10.9776/14403

Acknowledgements: The author thanks Jed Brubaker, Bonnie Nardi, and members of the Laboratory for Ubiquitous Computing & Interaction and EVOKE Lab & Studio.
Contact: cloder@uci.edu

1 Introduction

The participatory web came of age during a period of extreme market liberalization ushered in by passage of the Telecommunications Act of 1996, which has allowed for the proliferation of an astounding array of tools and services designed to facilitate communication and the sharing of data among networked individuals. The economic model used by most of these companies is to offer a free product or service to end users while selling targeted access to advertisers and third party developers (*e.g.* "Advertise on the Yahoo! Bing Network," n.d., "Advertise with Promoted Accounts · Twitter for Business," n.d., "Advertising on Facebook," n.d., "Facebook Platform Policies - Facebook Developers," n.d., "Google Ads," n.d.). This model incentivizes the commoditization of user data on the part of the platform developers, which frequently creates tension and confusion among users as they are confronted with advertising and algorithmically mediated content that reveals just how much access to their data web services have.

Notions of web security are frequently learned through storytelling among friends and acquaintances (Rader, Wash and Brooks, 2012). The rise of projects like CryptoParty, a decentralized collective attempting to make popular encryption tools more accessible to non-experts, suggests there is a growing interest in personal management of privacy and web security, and that there is a significant social component to the way these practices are learned. I argue that the growing use of encryption and other third-party privacy management tools in the United States are a reaction to the largely unregulated digital spaces that have become significant sites of social interaction; an effort on the part of users to instantiate a sphere of regulation at the level of the individual. This idea is further explored through an analysis of the early growth of CryptoParty, a decentralized collective of cryptography enthusiasts attempting to make encryption accessible to people outside the hacker community.

Grounded in an historical overview of telecommunications policy in the United States as it relates to the development of computer-mediated communication, I present a preliminary analysis of CryptoParty as a site where work of individual privacy regulation occurs, and is taught to others.

2 Regulation in U.S. Telecommunications

Telecommunications policy in the United States has been shaped almost entirely by two pieces of 20th century legislation: the Communications Act of 1934, and the Telecommunications Act of 1996. The former was built upon the assumption that it was in the public interest to operate the telephone network as a utility with universal access to all. Unlike many European countries, the U.S. did not adopt a model of state-owned telecommunications, instead opting for a regulated monopoly, seen as an economic necessity (Bauer, 2009). Constructing a physical telephone network to serve all Americans was a huge capital investment, and it was seen as an exchange in good faith for the government to allow AT&T to be the sole carrier, as long as universal access to phone service was provided (Aufderheide, 1999).

The sixty years following the passage of the Act of 1934 were a period of significant technological and social change, making the need for an update to the original legislation unavoidable by the 1990s. The advent of the internet and explosive popularity of the world wide web precipitated the convergence of technologies that had been regulated separately under the Act of 1934. The poor fit of the aging regulatory structure and the prevailing ideological disposition toward the benefit of competition in a free market system resulted in the highly deregulatory Telecommunications Act of 1996. A massive and complex piece of legislation, the Act's defining feature is the forbearance clause, which enacts a policy of *not* conducting or enforcing regulation that would interfere with the public interest[1]—the underlying assumption here being that a competitive marketplace will be of greater benefit to the public than a strictly regulated communications industry.

In the intervening years since 1996, advances in the development of web applications have created a complex ecosystem of services that position themselves alternately as platforms for public expression and as private businesses, dependent upon which is more convenient for the discussion at hand (Gillespie, 2010). As American users have begun to adopt the products of companies like Google and Facebook as methods of everyday communication, declining trust and comfort with the way these companies use customer data have become commonplace topics of conversation (*e.g.* Frum, 2012; Oswald, 2012; Paul, 2012). In the next section I discuss in more detail the way people are adapting their use of networked communication tools to align better with their personal interests.

3 The Rise of Individual Regulation

Brunton and Nissenbaum (2011) point out two asymmetries in the power dynamic of collecting user data on the web. First, that we are rarely able to *choose* whether or not to be monitored[2], nor do we have control over where that information goes or what happens to us because of it. Second, most often we do not know the full extent of the monitoring taking place. Nissenbaum (2009) asserts that there is no universal description of privacy for all people in all situations; that it is a highly contextual state dependent upon a multitude of factors, and that private vs. public is a false dichotomy. Palen and Dourish (2003) emphasize the dynamic and multidimensional nature of privacy as experienced by individuals managing presence in networked settings, drawing attention to the importance of taking into consideration broader social and institutional settings when discussing privacy concerns raised by new technologies.

Technological 'fixes' for privacy abound: numerous researchers and technologists have taken up the challenge to design and build technological tools that help people to manage and customize the visibility of their digital activity. Examples of such tools include PGP encryption for email (Garfinkel, 1994); Tor, which allows for anonymous browsing by routing traffic through multiple nodes in a secure network (Tor Project,

[1] A term of art in the policy sphere, 'public interest' has notoriously defied stable definition (Krasnow & Goodman, 1997; Schultze, 2008), yet has been a central characteristic of U.S. communications policy since the 1927 Radio Act.

[2] Brunton and Nissenbaum reject the plausibility of the argument that a user can opt out of using a service if they are uncomfortable with the data capture policy (as does Portwood-Stacer, 2012), and I agree. While technically possible, there is often a substantial social cost to withdrawing from these services.

n.d.); and more recently, TrackMeNot, a browser plugin designed to obfuscate internet activity in order to confound tracking cookies (Howe & Nissenbaum, 2009) Despite the proliferation of tools and the increasing sophistication of privacy settings built into commonly used apps and services, they have repeatedly been shown to be difficult for users to configure and implement as desired (boyd & Hargittai, 2010; Sheng, Broderick, Koranda, & Hyland, 2006; Whitten & Tygar, 1999).

To use Brunton and Nissenbaum's (2011) terminology, growing awareness of these tools has resulted in an increasing amount of *vernacular resistance* to the economic model of data capture. Methods of vernacular resistance entail individuals engaging in small acts of subversion to better align their use of a system with their personal tolerance for data collection. In the sections below I discuss first the experience of developing data management strategies from an individual perspective, followed by the creation of CryptoParty, a global effort to provide people the skills to decide upon and engage in their own forms of vernacular resistance.

3.1 Individual Data Management

Greg is an American is in his late twenties with a bachelors degree in information technology from a large public university. In the fall of 2011 he became involved with the Occupy movement, participating in protest activity in a major American city over a span of several months. Given this experience, his perspective on the use of encryption is likely more sophisticated than the typical internet user because he has developed tactics not only for managing his own digital presence, but was also an active participant in the development of information security strategies within the Occupy movement.

While he has always been interested in computers and computing, Greg was a relative latecomer to the participatory web. Until 2010, he identified himself primarily as a lurker; someone who would surf the web, observing and consuming information but not creating any content. During this time he was not a member of Facebook or other social netowrk sites, and describes the extent of his internet activity as "surfing cool websites, looking at interesting videos and just using email."

When WikiLeaks gained publicity in 2010 over the release of U.S. State Department diplomatic cables, Greg was curious about the technology that made such a thing possible. It was at this point that he first learned about Tor and PGP encryption, which are used to anonymize traffic within a network and scramble the content of messages, respectively. Motivated politically and by his interest in the technology, Greg became involved in the community of hackers developing, using, and advocating for encryption. With the knowledge gained through this involvement and the tools at his disposal to have more control over his web presence, Greg became much more active online. Today he uses Facebook, Twitter, and maintains a blog. He uses some form of encryption (or where not possible/plausible, obfuscation) with each of these tools.

He clearly differentiates between security and anonymity, and the realistic possibilities for each when using computer versus a mobile device. Because he uses Twitter on his smartphone, which carries a regulatory legacy that his laptop does not, his service provider and the government are able to connect that activity to his legal identity.

> Because I use twitter on my Android device, [the government] knows exactly who I am, especially because I'm involved in [Occupy]. …and in a way, this is kind of a learning experience for me because…if I really wanted to maintain some anonymity, I would go about it in a completely different way, which would involve a complete new set of practices.

He has decided that this possible disclosure of his legal identity is an acceptable level of risk, and proactively manages this potential risk by self-regulating what he posts to Twitter. Anything considered especially sensitive is sent through other, usually encrypted, channels. It is through this active, conscious process of managing multiple data streams that Greg is able to fill in regulatory gaps (in his perception and

expectation) in order to make his digital activity visible to only the audience he intends. In the absence of policy defining a boundary, he is creating and policing his own.

3.2 CryptoParty

Boullier acknowledges the common perception among developers and technologists that users are generally unwilling to adopt new practices, but also asserts that "users are in fact ready to go to remarkable lengths to adapt their ways of doing things, providing they are…given clear, decisive and reliable instructions" (2001, cited in Boullier, Jollivet, & Audren, 2007 p. 1278). CryptoParty is one example of a community-based effort to provide such instruction for people interested in learning how to use basic encryption tools.

On its wiki, CryptoParty defines itself as "interested parties with computers, devices, and the desire to learn to use the most basic crypto programs and the fundamental concepts of their operation! CryptoParties are free to attend, public, and are commercially and politically non-aligned." Gatherings are organized ad hoc by volunteers in each city; as of this writing, there have been more than 100 gatherings on five continents since the first was held in Australia in August 2012 ("CryptoParty," n.d.). It is noteworthy that one of the first things mentioned in a statement about how to contribute is the request to "use language and methods an absolute newbie can understand" ("CryptoParty Handbook," n.d.). This openness to non-experts is not something that geek and hacker communities are known for (Coleman, 2012), and could be indicative of a larger cultural shift in these groups as privacy and surveillance become more quotidian concerns.

To date, this research has focused primarily on CryptoParty as an organization. The next phase of this project will include fieldwork at CryptoParty gatherings to better understand the motivations and experiences of non-experts as they learn to take a more active role in their personal data management.

4 Conclusion

In this paper, I have traced the history of policy decisions that have shaped the current market-driven landscape of communication in digital spaces, and described how technical solutions designed to address privacy concerns in these spaces have been largely unsuccessful in attracting users. CryptoParty has been presented as a case where people with knowledge of current privacy management tools are reaching out to help those with less expertise. This outreach expands not only the reach of these tools, but awareness of the options available for privacy management among the general public.

I argue that individual management of digital exposure and concealment can be conceptualized as an instantiation of micro-regulation in the absence of regulation at the national (or international) level. This paper does not address whether regulation at a higher level would negate the perceived need for third party privacy management, nor whether similar activity is happening outside the United States, but these are important questions for consideration in future work. This paper does illustrate strategies by which individual users are beginning to take control of their personal data management, and how CryptoParty has developed as a way to overcome longstanding usability hurdles for third party privacy management tools, particularly encryption.

This is a preliminary description of the actions taken by individuals in response to discomfort or disagreement with the practices of data capture performed by most major platforms of communication on the internet. My intent is to open discussion about privacy to interests and agents outside the usual suspects of governments and corporations; to investigate how privacy and security are negotiated at a human scale.

5 References

Advertise on the Yahoo! Bing Network - Bing Search Advertising. (n.d.). Retrieved November 28, 2012, from http://advertise.bingads.microsoft.com/en-us/home

Advertise with Promoted Accounts · Twitter for Business. (n.d.). Retrieved November 28, 2012, from https://business.twitter.com/en/advertise/promoted-accounts/

Advertising on Facebook | Facebook. (n.d.). Retrieved November 28, 2012, from https://www.facebook.com/about/ads/

Aufderheide, P. (1999). "Background", "The Shaping of the Act", and "Overview of the Act." In *Communications Policy and the Public Interest: The telecommunications Act of 1996*. New York: Guilford Press.

Bauer, J. (2009). Transformations of the state in telecommunications. *Available at SSRN 1418215*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1418215

Boullier, D., Jollivet, P., & Audren, F. (2007). Security: always too much and never enough Anthropology of a non-starter market. *Annals of Telecommunications*, *62*(11), 1274–1292.

Boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares. *First Monday*, *15*(8), 2.

Brunton, F., & Nissenbaum, H. (2011). Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday*, *16*(5). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3493

Coleman, E. G. (2012). *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton University Press.

CryptoParty. (n.d.). Retrieved October 12, 2012, from https://cryptoparty.org/wiki/CryptoParty

CryptoPartyHandbook. (n.d.). *cryptoparty.org*. Retrieved December 4, 2012, from https://cryptoparty.org/wiki/CryptoPartyHandbook

Facebook Platform Policies - Facebook Developers. (n.d.). Retrieved November 28, 2012, from http://developers.facebook.com/policy/

Frum, D. (2012, August 7). Facebook needs to earn your trust. *CNN Opinion*. Retrieved from http://www.cnn.com/2012/08/06/opinion/frum-facebook/index.html

Gillespie, T. (2010). The politics of "platforms." *New Media & Society*, *12*(3), 347.

Google Ads. (n.d.). Retrieved November 28, 2012, from http://www.google.com/ads/adwords2/#tab-3

Krasnow, E. G., & Goodman, J. N. (1997). Public Interest Standard: The Search for the Holy Grail, The. *Fed. Comm. LJ*, *50*, 605.

Oswald, E. (2012, March 1). You can trust Google to spy on you. *betanews.com*. Retrieved from http://betanews.com/2012/03/01/you-can-trust-google-to-spy-on-you/

Paul, I. (2012, May 15). Facebook Users Don't Trust Site on Privacy Issues. *PC World*. Retrieved from http://www.pcworld.com/article/255615/facebook_users_dont_trust_site_on_privacy_issues.html

Portwood-Stacer, L. (2012). Media refusal and conspicuous non-consumption: The performative and political dimensions of Facebook abstention. *New Media & Society*. doi:10.1177/1461444812465139

Rader, E., Wash, R., & Brooks, B. (2012). Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 6). Retrieved from http://dl.acm.org/citation.cfm?id=2335364

Schultze, S. (2008). *The business of broadband and the public interest: Media policy for the network society*`. Massachusetts Institute of Technology. Retrieved from http://www.scribd.com/fullscreen/146381135?access_key=key-26l9as49j8xibfzhj50y&allow_share=true&view_mode=scroll

Sheng, S., Broderick, L., Koranda, C. A., & Hyland, J. J. (2006). **Why Johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security*. Retrieved from http://chariotsfire.com/pub/sheng-poster_abstract.pdf

Whitten, A., & Tygar, J. D. (1999). **Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium* (Vol. 99). Retrieved from http://www.usenix.org/events/sec99/full_papers/whitten/whitten.ps