Defining the Line of Personal Data Privacy

L. Joseph Pratt
University of Tennessee Chattanooga
CPSC 3610

Blurry is the line between private and public data. The internet is a new kind of public since one can interact with data or people on the other side of the planet. The U.S. Citizen must reflect on the Fourth Amendment and develop a reasonable expectation of privacy as policy makers and interpreters define the laws concerning the digital landscape.

Introduction

The digital age is fully upon us. The digital medium has fully integrated into the lives of most U.S. Citizens. Computers invisibly connected to other computers easily fit in our pocket. These small devices are blindingly faster than massive room-size computers considered cutting-edge not too many years ago. In a blink of an eye, we have caught up with what Science Fiction writers merely dreamed about a few decades ago.

Laws concerning the proper use of computers have been painfully slow to update. Coupled with a national crisis on 9/11, the government or any company with the funds to swing it has had unprecedented access into the lives of individuals throughout this country, both citizen and non-citizen [1].

Particularly in light of the information revealed about the NSA's actions to tap into these mass computer networks, one must reevaluate the issue, even the necessity, of defining the line of personal data, who has access to it and how and when that data is accessed [2].

Privacy of a U.S. Citizen

Like a footprint in the sand, or markings on a scrap of paper, each user of the internet, whether by phone, personal computer or tablet leaves his or her mark. Unlike a footprint in the snow that fills with flakes and disappears, the break-neck pace of computer advancement now allows one's digital footprint to linger indefinitely. Moreover, the rights of ownership of those bits are currently in an incompletely defined gray area. The user of the service may store personal data on a remote server owned by another company. Whose bits are they? The manipulator (the user) or the storer (the server owner)?

Regardless of who owns them, however, it is clear that the information contained in the interpretation of those bits do indeed belong to the user.

The thrust of the Fourth Amendment is to protect the U.S. Citizen from unreasonable searches and seizures of his or her "persons, houses, papers, and effects [3]." Though written over 200 years ago, the U.S. Supreme Court has continually interpreted the Amendment to ensure that citizens' privacy is protected [4].

Originally, the roots of the Fourth Amendment come from the colonial days of America. British authorities made use of general warrants known as "writs of assistance" that essentially gave unlimited permission for custom agents and the like unimpeded access into the homes of the colonists. This allowed tax collectors to search and collect prohibited and uncustomed goods, regardless if they were truly such. The abuse of general warrants was a key precipitant that solidified sentiments in favor of the Revolutionary War [5].

In 1967, the U.S. Supreme Court further interpreted the Fourth Amendment to extend to personal privacy as well. In the case Katz v. United States, the Supreme Court ruled that it was unconstitutional for law enforcement to listen in on a conversation held in a phone booth. The court found that when a person enters a phone booth to hold a conversation, he has a reasonable expectation to privacy that the conversation will not be "broadcast to the world." [4] Therefore, even something intangible like an audible conversation is protected because of the *reasonable expectation of privacy*.

Personal Data and "Paper and Effects"

So, how does this relate to the digital footprint on the internet? When someone writes an email, leaves a voice message, or engages in a private online chat, that individual

has a reason to believe that these interactions will be kept private. Moreover, if a user performs a simple search on a popular web service, there is no apparent tie with the person performing the search. He or she provides no personal information tied to the service. The user has a reasonable expectation to privacy. However, this person's "papers and effects" no longer reside in his or her home or personal digital device. They have moved out into a kind of pseudo-public place that is even more difficult to define. More importantly, with the capabilities of analyzing large sets of data, what was once thought to be private data is now personally identifiable data [6].

A Different Kind of "Public"

The internet is a revolutionary new kind of "public". Never before in human history has an individual been able to write information remotely and in real-time. A person can hold a small device in his or her lap and manipulate the physical state of a hard drive potentially thousands of miles away - nearly instantaneously. Someone can join a public chat room and interact with others with common interests while lying in bed.

Historically, sending written information was non-public. If a family member wanted to communicate with a loved one in some faraway place, he or she would need to pen a letter and send it. The information would physically move from one location to another. The receiver of the letter could then keep it or destroy it, and no one would be able to view it without his or her permission.

Even using a telephone, the voice signal that was transmitted electronically terminated in the earpiece of the phone at the other end of the connection. Without some recording device, the transmitted electronic signal would dissipate as sound waves into the air never to be heard again.

Now, human interactions with one another and other digital mediums can potentially be preserved forever. Couple that with the "cloud" and now everything one does and says resides somewhere out "there" and he or she has no real control over who has access to the data.

Shaping the Internet

The spread of the internet is reminiscent of how the West was settled. Any rules guiding proper use of the virtual landscape are difficult to define, and approaching impossible to enforce. The potentially limitless nature of the internet feels, to many, as it probably felt to travelers moving across the Great Plains, open and wild – offering freedom and newness to anyone. However, in the case of the internet, the computer scientist (or anyone involved) can shape the landscape of the internet to fit whatever structural paradigm he or she wishes to impress upon it.

To avoid the mistakes of the lawlessness of the west, to protect the common user of the internet, privacy protocols should become standard. If a series of bits can be a number, or a word, or a CPU instruction, then so a bit or series of bits can identify data as private. With this, those shaping the internet can clearly define and potentially protect that which is "mine" and that which is "yours", with the proper controls in place.

Conclusion

To preserve that which is essential to the identity of a U.S. Citizen, influential individuals such as prominent computer scientists, lawmakers, and thought-leaders should make strides to shape the future of digital privacy. Like a vector graphics line, those influential ones must clearly define the answer to "What is private data?" so no matter how closely one "zooms in," the line between that which is private and public is clearly

distinguishable. With the line clearly defined, lawmakers and law enforcement agencies can properly define and use the "papers and effects" of this new age.

Bibliography

[1] Ahmadi, Shafiqa. “Giving the U.S. a Bad Reputation”. http://www.nytimes.com/roomfordebate/2011/09/07/do-we-still-need-the-patriot-act/the-patriot-act-gives-the-us-a-bad-reputation. September 8, 2011.

[2] Electronic Frontier Foundation. “NSA Spying on Americans”. https://www.eff.org/nsa-spying. Accessed 11/25/2013.

[3] The Bill of Rights. http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html.

[4] Casebriefs. “Katz v. United States”. http://www.casebriefs.com/blog/law/criminal-procedure/criminal-procedure-keyed-to-saltzburg/searches-and-seizures-of-persons-and-things/katz-v-united-states-3/. Accessed 11/25/2013.

[5] Sparknotes. “The Writ of Assistance”. http://www.sparknotes.com/history/american/prerevolution/section3.rhtml. Accessed 11/25/2013.

[6] Barbaro, Michael. Zeller,Tom. “A Face Is Exposed for AOL Searcher No. 4417749”. http://www.nytimes.com/2006/08/09/technology/09aol.html?ei=5090&en=f6f61949c6da4d38&ex=1312776000&partner=rssuserland&emc=rss&pagewanted=all&_r=0. August 9, 2006.