DIGITAL PRIVACY: THINK TWICE BEFORE YOU TWEET!

Claire R. La Roche, Longwood University, 201 High Street, Farmville, VA 23901

ABSTRACT

An important social and legal issue with significant personal and professional implications is the scope of the right of privacy associated with digital communication. Privacy is an important guardian of free speech – one of the critical elements promoting creativity. In the spring of 2013, the author conducted the Digital Privacy Survey of 103 undergraduate students and the results of the survey are analyzed. The limitations of the Electronic Communications Privacy Act (ECPA) are discussed and amendments to this law are proposed. Suggestions are also made for minimizing the unintentional sharing of personal information.

Introduction

Data collection begins the moment a computer is turned on. Each online search, website encounter and email generates personal information that the user may be unconsciously revealing. With the ubiquitous camera-phone, subjects are frequently unaware that they have been photographed until their image appears online. Additionally, daily social interactions are both voluntarily and inadvertently shared through Twitter, Instagram, social media, text messages and email.

There are significant limitations to privacy rights attached to digital communication stored at least 180 days. To ensure that digital information is stored and thus more accessible, the National Security Agency (NSA) is currently constructing an enormous Data Collection Center in Utah and another analytics facility in North Carolina. [Biesecker, 2013] Some experts estimate that the Utah facility will be capable of storing 5 zettabytes of information – every digital footprint in the world for a very long time [Berkes, 2013]. In the wake of the NSA's Prism program and internal auditor's recent revelations that the NSA has violated privacy laws thousands of times a year since 2008 [Gellman, 2013], users of digital technology should be acutely aware that digital information is stored and at times, illegally seized. Innumerable regulations and obscure laws combined with the outdated ECPA and new governmental data warehouses, creates legitimate concerns.

Digital Footprint

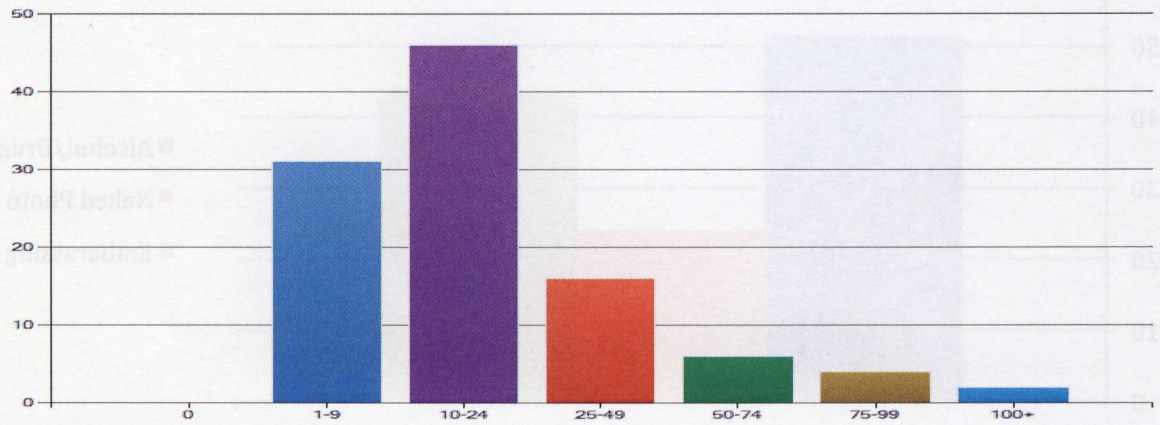
There are several misconceptions about the privacy of digital technology including, but not limited to, text messages, email, and social networking. The Internet does not have a delete button and when asked in the 2013 Digital Privacy Survey, 40% of respondents were unaware of the permanent nature of Internet activity. Only 36.19% were aware of the massive NSA data collection and storage facilities.

In the digital age, new methods of communication and living life in the public eye are developing at a rapid rate. According to the 2013 Digital Privacy Survey, 94.1% of survey respondents had an ever-present Smart phone -- essentially a mini-computer and mother lode of personal information. Although e-mail, text messages, Twitter and Facebook may provide an efficient means to communicate and chronicle life events, they are generally used without time to reflect on the potential consequences. Some of the common ways that a daily narrative is digitally recorded is revealed in the aforementioned survey of 103 students. The 2013 Digital Privacy survey indicates that 62.9% have a Twitter account, 95.2% have a Facebook page, and 99% have a laptop. Survey results also indicate the extent to which the students are digitally connected. On a daily basis, all of those surveyed use email, 98.1% text message, and 82.8%

access Facebook. Approximately three fourths of the Facebook users access their account multiple times a day.

As Figure 1 illustrates, 100% of the survey respondents search the Internet on a daily basis. Every time an email is sent or an app is bought, personal information is shared and sold to others. Collecting, selling, sharing and data mining personal information are commonplace and Internet users participate in these pursuits without due consideration of privacy.

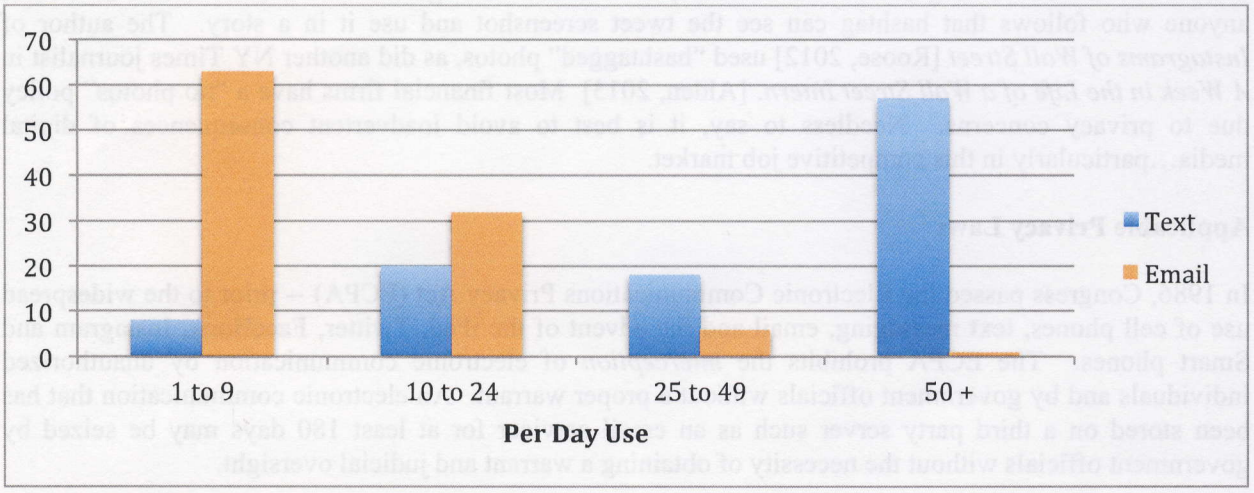
Figure 1. Students (%) and Number of Daily Internet Searches



Source: La Roche 2013 Digital Privacy Survey

E-mail messages are informal and are frequently sent without much consideration of the contents. Text messages are even more instantaneous and are commonly sent with even less reflection than an email. The 2013 Digital Privacy Survey indicates that among respondents, text messages are now a more frequently used communication tool than email and the results are shown in Figure 2. In a typical day, 63 of respondents (60%) said that they use email between 1-9 times and 57 students (54%) use text messaging 50+ times a day.

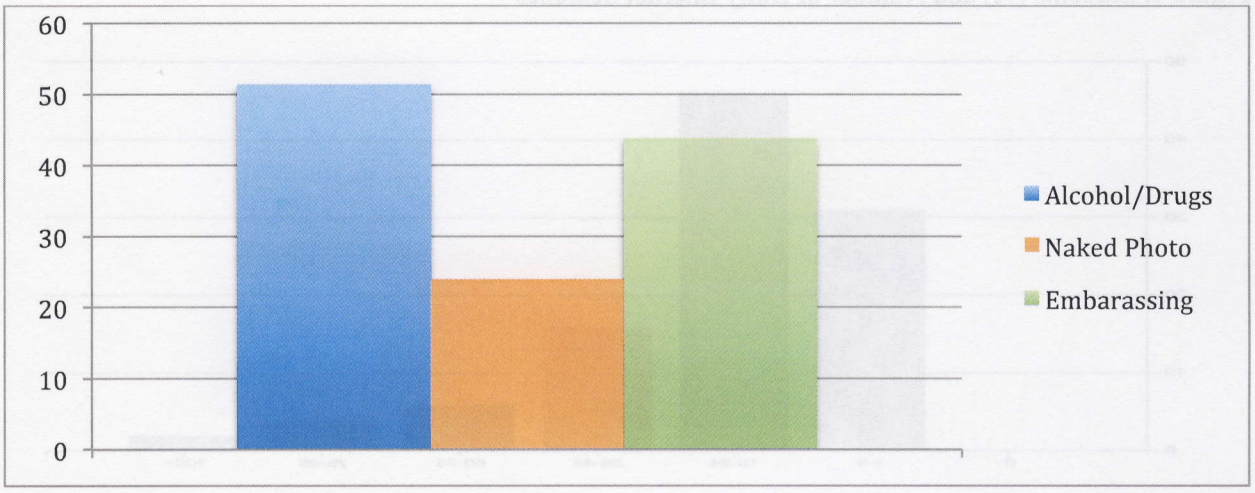
Figure 2. Students and Daily Use of Text versus Email



Source: La Roche 2013 Digital Privacy Survey

Due to the immediate and casual nature of text messages, tweets and other forms of digital communication, users frequently post inappropriate personal information. Figure 3 shows that 43.8% of the survey respondents indicated they have posted, tweeted or texted digital content that they consider embarrassing and would not want a prospective or current employer to view. The survey responses also indicated that 23.8% have had photos posted or sent in which they are partially or completely unclothed and 51.4% have had photos drinking alcohol or using an illegal substance digitally communicated.

Figure 3. Embarrassing Digital Content (percent)



Source: La Roche 2013 Digital Privacy Survey

"Hashtags" Enlarge Footprint

Twitter is growing in popularity and 62.8% (66) of the respondents "tweet" -- over half on a daily basis (51%). A Twitter user may think that only their known followers on Twitter have the ability to see their tweets. In reality, if a tweet or Instagram (a popular photo sharing/social networking site) is hashtagged, others including savvy journalists and financial firms can see it. According to one business journalist who declined to be named, "There are hundreds, if not thousands of journalists trolling Twitter. Every journalist uses TweetDeck and a lot of financial firms are Twitter savvy and follow what people say about them on social networking sites." For instance, if an intern hashtags a Tweet with the name of a firm, anyone who follows that hashtag can see the tweet screenshot and use it in a story. The author of *Instagrams of Wall Street* [Roose, 2012] used "hashtagged" photos, as did another NY Times journalist in *A Week in the Life of a Wall Street Intern*. [Alden, 2013] Most financial firms have a "no photos" policy due to privacy concerns. Needless to say, it is best to avoid inadvertent consequences of digital media…particularly in this competitive job market.

Applicable Privacy Laws

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) -- prior to the widespread use of cell phones, text messaging, email and the advent of the iPad, Twitter, FaceBook, Instagram and Smart phones. The ECPA prohibits the *interception* of electronic communication by unauthorized individuals and by government officials without a proper warrant. An electronic communication that has been stored on a third party server such as an email servicer for at least 180 days may be seized by government officials without the necessity of obtaining a warrant and judicial oversight.

The following are some of the fundamental changes that have been made since the analog age of 1986 morphed into the digital age:

- **Email** -- Although Title I of the ECPA protects electronic communications while in transit, after email messages have been stored on a server for at least 180 days they are deemed "abandoned" and law enforcement may obtain these communications without the necessity of obtaining a warrant and an accompanying judicial review. The only requirement is a statement that the communication may be relevant to an investigation. This is pertinent because at the time the ECPA was signed into law, electronic communication was stored on a third party server for a brief period of time -- just long enough for it to be transferred to the customer's email account. Today, Hotmail and Gmail users may store email online or the third party server may store digital communication indefinitely. The new NSA Data Collection Center will insure that these digital communications are stored on a third party server.
- **Social Networking** – Facebook was not established until 2004, eighteen years after the adoption of the ECPA. The omnipresent digital camera and the use of Facebook, Twitter and Instagram encourage users to live daily life in the public eye.
- **"The Cloud"**-- Saving digital information and files in "the cloud" provides users with the ability to store massive amounts of data and at the same time the cloud facilitates collaboration.
- **Smart phones** – Smart phones are essentially mini-computers with built-in GPS. The location data generated by a Smart phone is stored and can readily be accessed. Employers frequently provide employees with Smart phones. The ECPA has never prohibited employers from accessing an employee's electronic communication in the workplace when one of the parties consents, when the employer is providing the service, or when monitoring is done in the ordinary course of business. Thus, employers may legally access most, if not all, of the employee's personal communications and movements. With minimal effort, the government has access to the same information.

Based on the rationale of national security, Internet service providers (ISP) are being pressured by the NSA, FBI, IRS and the Executive Branch to reveal subscribers' digital activity. [Miller, 2013] Google freely admits that users do not have a reasonable expectation of privacy with Gmail. In part, this is because users signed up for this service agreeing to contextual advertising based on searchable email. [Wood, 2013] In a court motion to dismiss a class action accusing Google of violating the ECPA, Google's executive chairman, Eric Schmidt admitted that "Google policy is to get right up to the creepy line and not cross it." [Rushe, 2013] To make matters worse, there is a dearth of federal court decisions applying the Fourth Amendment to digital technology. For instance, the US Supreme Court has not specifically weighed in on privacy rights associated with stored text messages.

Conclusion

The mass surveillance of US citizens undertaken by the NSA combined with the enormous data collection and warehousing facility coming on line in Utah presents an affront to freedom of speech and personal privacy. The ECPA and court decisions provide that: (1) Employees have no reasonable expectation of privacy regarding electronic communications and should consider all digital communications sent on their company's system to be legally accessible and (2) Once any digital communication has been stored for 180 days, it may be accessed by the government without the necessity of a warrant.

Senator Mike Lee along with Senator Patrick Leahy, one of the original sponsors of the ECPA, recently introduced legislation to require a warrant prior to the seizure of stored electronic communication. "The ACLU, along with Google, Microsoft, Yahoo and Facebook, are all lobbying Congress to revise the ECPA, according to their most recent lobbying disclosure reports." [Sasso, 2013]

Amendments to the ECPA should be clear, simple and consistent and include the following:

- Preservation of the applicability of the Fourth Amendment and search warrant requirements for access to private communications.
- Internet Service Providers only have to reveal stored communications after a search warrant has been provided.
- Communication should be protected without regard to age, whether it is in transit or stored, opened or not.

It is almost impossible to avoid using digital technology. We should all be aware of the permanent nature of our digital footprint and keep in mind the lack of privacy protection. Scanning and reading personal and private email is an ordinary business practice for Google and others. If email users want to avoid the routine scanning of the contents of their email, they should avoid using the free email services of providers such as Gmail and Hotmail. Due to the propensity to digitally chronicle daily life, students should set their Twitter account to private and perhaps remove their Facebook page before applying for a job. Interns should avoid using hashtags -- unintended followers can and will see their Instagrams and Tweets.

REFERENCES

[1] Alden, W. (2013). *A Week in the Life of a Wall Street Intern*. Retrieved from http://dealbook.nytimes.com/2013/06/07/a-week-in-the-life-of-a-wall-street-intern/

[2] Biesecker, M. (2013). *NC State-NSA partnership may help analyze Utah data*. Retrieved from http://www.sltrib.com/sltrib/world/56739756-68/data-nsa-state-research.html.csp/

[3] Berkes, H. (2013). *Amid Data Controversy, NSA Builds Its Biggest Data Farm.* Retrieved from http://www.npr.org/2013/06/10/190160772/amid-data-controversy-nsa-builds-its-biggest-data-farm/

[4] Electronic Communications Privacy Act, 18 USC, §§2701-12

[5] Gellman, B. (2013). *NSA broke privacy rules thousands of times per year, audit finds*. Retrieved from http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html/

[6] Miller, C. (2013). *Secret Court Put Tech Companies in a Data Bind*. Retrieved from http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-data-bind.html?pagewanted=all&_r=1&/

[7] Roose, K. (2012). *Instagrams of Wall Street.* Retrieved from http://nymag.com/daily/intelligencer/2012/07/instagrams-of-wall-street.html/

[8] Rushe, D. (2013). *Google: Gmail users shouldn't expect email privacy*. http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit/

[9] Sasso, B. (2013). *Facebook, email providers say they require warrants for private data seizures*. http://thehill.com/blogs/hillicon-valley/technology/279441-facebook-email-providers-require-warrants-for-private-data-seizures/

[10] Wood, M. (2013). *Gmail: You weren't really expecting privacy, were you?* http://news.cnet.com/8301-31322_3-57598424-256/gmail-you-werent-really-expecting-privacy-were-you/