The Price Of Privacy: An Examination of the Economic Costs of Abstention from Social Networks

Greg Norcie
Center for Democracy & Technology

L Jean Camp
Indiana University

Abstract

Currently the common school of thought is that individuals either choose to participate in social networks, at the expense of their privacy, or choose to abstain from said social networking sites (SNSs.) We illustrate in this paper that there are very real costs and risks to not participating in social networks. The analysis we provide here illustrates that not participating in social networks is likely to have a significant career cost, and thus that expecting privacy sensitive users to abstain from social networking may not be reasonable. If users face harm whether or not they use SNSs, the rational choice is to join a SNS and gain the utility of SNS membership. Specifically, we delve into the risks associated with *abstaining* from social networks, enumerate the *risks* encountered when participating in SNSs. We conclude that a rational actor would elect to participate in social networking; and that this choice cannot be accurately described without assessment of the considerable negative externalities.

1 Introduction

One common criticism levied at privacy advocates is that no one is forced to join a social networking site (SNS). Within this statement is the implication that users who do not wish to have their privacy violated should simply abstain from social networking, and that the only cost to the user is the inability to access said social network. In this paper, we will discuss the reasons that this is a flawed argument. We will discuss that non-participation in social networking also carries significant risks, while conversely, electing to join a SNS confers economic benefits. We will discuss the fact that data often remains on social networks upon deletion of individual posts and/or deletion of entire SNS profiles. Thus, a user who is upset by a privacy policy change can not mitigate harm by deleting information nor leaving said social network. In addition, we discuss how those who abstain from social networks risk reputational harms, such as impostors creating malicious social networking profiles. Finally, we will discuss the specific economic harms encountered when abstaining from social networking. (For example, higher prices due to lack of information available to price discrimination algorithms). We also discuss the fact that social networking, like traditional offline networking, can influence hiring and salary decisions. This paper continues along three points. Firstly, we discuss the *benefits* of participating in social networks. Then, we will discuss the risks associated with *abstaining* from social networks. Thirdly, we will discuss the risks of participating in social networks. Finally, based on our analysis, we will discuss how the economic disadvantages facing SNS abstainers, coupled with the fact that abstaining from SNSs also carries risk has implications for public policy regarding SNS privacy rights.

2 Benefits of Participation

Networking in the context of this paper refers not to transit of bits, but rather making social connections for business purposes. Networking is a central concept in career building. Networking leads to greater opportunities, including higher paying jobs, and high paying positions within companies. Literature from sociology backs up this practice, showing that "weak ties" (i.e. old school mates, former coworkers, friends of friend etc.) are known to be important for obtaining jobs and/or promotions [19]. Social networking websites (SNSs) afford many new and useful avenues for networking. SNSs like LinkedIn and Facebook reduce the time and effort needed to reconnect with "dormant ties". Levin et al [23]. defined dormant ties as persons who had not been contacted in the past 3–5 years, and found that reconnecting with dormant ties can aid job searches. Levin et al. also point out that the ability of social networking to aid this strategy can have a negative effect as well,

incentivizing workers to make many quick, shallow connections. Note that a common criticism of online SNS is that they encourage formation of many quick, shallow connections (exactly those that Levin indicates are strategic). Not only can networks can get people jobs, but also lack of networks can deny opportunities. As Metcalfe's Law point out, the strength of a communications network is equal to the number of its users squared (n^2). DiMaggio and Garip [14] elaborated along similar lines, examining how network externalities can increase income inequality. DiMaggio and Garip point out that if a good, service, and/or practice influences life chances, and that good, service, and/or practice is characterized by network externalities, then these network effects can exacerbate economic inequality. Recall that network externalities occur when one person's adoption of the good increases the benefit to other adopters of the good. That is, the value I receive from a product with network externalities increases as more people also adopt said product. Two classic examples cited by DiMaggio and Garip are telephony adoption and Advanced Placement exams.[1] As DiMaggio and Garip point out, the first private telephone line was purchased by a Palo Alto hardware store owner in 1892, however, the telephone did not reach 90% penetration in the United States until 1970. This was because of the expense of telephony, and thus only business owners wishing to coordinate purchases used them. Not only was there not enough of a positive network externality for personal use; but in fact AT& T had public relations campaigns discourage frivolous use [16]. Similarly, students in US high schools with large AP classes benefit from positive network externalities such as the ability to study in groups, collaborate on homework, share expensive equipment such as scientific calculators. Thus, when network externalities are positive, you adopt. If your school has large AP classes, you are more likely to take the AP exam. If your friends all have telephones, the telephone network is more valuable. And if your friends all use a social network, you are more likely to use that social network. Social networks have been shown to assist displaced employees in employment searches. Cingano and Rosolia [12] did a study focused on workers who entered unemployment due to firm closures. Their data comprised of 13 million employment relationships and 1.2 million employment histories between 1975 and 1997 in two Italian provinces. Cingano et al. found that the higher employment rate in one's social network is positively correlated with likelihood of finding employment. However, there are limits to positive network effects. A model created by Beaman [6] showed that the relationship between the size of one's social network and employment outcomes is non-monotonic. Past a certain point, having additional members in a social network can decrease job prospects, since there are only a finite number of jobs. Using social networks carries risks as well as potential benefits. Users may accidentally reveal information they wished to keep private. Moving on, we will detail some potential risks that failing to create a social networking profile creates, as well as the risks inherent in possessing a social networking profile.

[1] Advanced Placement (AP) exams allow United States students to receive college credit for classes taken in high school. AP tests are typically only offer for free in public schools in affluent areas.

3 Risks of Non-Participation

While much literature (aside from this paper) has focused on the risks associated with participating in social networks, little work has been done on the risks associated with abstaining from social networks. In addition to failing to incur benefits when using social networking, there are also risks association with abstention from social networking. In this section we identify three main risks of abstaining from social networks: The first risk is the inability to review and/or report information posted about oneself. SNS can serve as invisible transmitters of misinformation to those not participating. The second is the threat of impersonation. The third, based on studies of reputation systems and human trust, is the risk of being perceived as untrustworthy.

3.1 *Tagging and Talking*

Abstaining from SNSs does not prohibit others (friends or not) from posting about an abstainer on social media. Abstaining does prohibit one from reviewing the posts in which one is tagged or identified. For example, unique recognition is enabled by tagging and facial identification; neither requires participation in the SNS. Malicious tagging has been well-documented[35]; miscreants can tag users in unflattering or embarrassing photographs, as well as erroneously tag users, either by accident or with malicious intent. For example, individuals can tag a photo as an elephant to insinuate the abstainer is overweight. Thus users face a dilemma. Joining a SNS enables reviewing posts about them, but there is a loss of privacy in the process. Those abstaining risk rude, embarrassing, and/or libelous information being posted about them without their knowledge. While the user may not see these photos, others can (including, possibly, those in a position of authority over the abstainer.)

3.2 *The Risk of Impersonation*

Another risk faced by SNS abstainers is the risk of impersonation. Abstaining from social networking (or setting privacy settings in such a way that the general public

cannot see your profile) leads to a risk of impersonation. Major social networks such as Facebook and Twitter do not verify that an account creator is in fact, the person the account claims to be. If a user opts to not register for a given social network (or hides a personal profile from search), a malicious attacker could impersonate that user. For example, alleged Sandy Hook shooter Adam Lanza's brother was impersonated on Facebook. This fake account then proceeded to give a slanderous interview to the New York Post [15]. Thus, in addition to having rude information posted *about* a SNS abstainer, malicious attackers could create an account pretending to *be* the abstainer. This account could be used to phish the abstainer's social network, or to embarrass the abstainer by posting socially unacceptable text and/or images to the social network.

3.3 *Without Data, Comes Consequences*

In addition to the risk of impersonation, users without a social networking profile fail to generate the "social signal" that many organizations use when evaluating risk and pricing. When someone requests a loan, a bank evaluates the applicants credit score to see if that person is a trustworthy individual. Depending on one's credit score, a loan may be denied, or it may be granted but at a much higher interest rate. Persons without a credit history, and thus without a credit score, can find it difficult to secure loans. In the absence of a credit history, no expectation of trust can exist. Similarly, persons without a social media presence may suffer from a perceived lack of history. As Friedman and Resnick illustrated [17], new pseudonyms or identities without histories are perceived as untrustworthy. And as reporter Kashmir Hill has noted, many employers now examine social media when evaluating applicants, and the lack of social media accounts can be seen as suspicious to potential employers [20]. Further, services which quantify social capital, like Klout [21], use social media interactions as the signal for their algorithm. With the proliferation of these tools, those who abstain from social media also risk being (potentially falsely) branded as lacking status or influence. This can have a very real economic cost. Influential Klout users are often offered special deals, in hopes they will evangelize a company's products and/or services. And in the field of advertising or journalism, Klout score may be factored in during hiring decisions [28]. Outside the realm of business, social media abstainers could find seemingly basic tasks complicated. Many websites allow users to log in with their social media account, and not all of them allow a user to instead opt to create a site specific login. Furthermore, some sites even allow users to link their SNS profiles to enhance trust[3, 26]. Thus, without the data from a "social signal", many pricing algorithms may raise prices for SNS abstainers. Previous work by Böehme et al. [7] has described privacy as a luxury good, pointing out that price discrimination is muddled by privacy enhancing technologies, and that in the absence of data usable for price discrimination, prices may rise across the board. He illustrates that when such data are available, PET users will pay higher prices. Not sharing information can have a price, in a world where tracking is widely used for price discrimination [27]. Having detailed the major threats from failing to create a social media profile, the next section will detail some of the risks inherent in social networking, demonstrating the dilemma faced by users debating creation of a social networking profile.

4 Risks of Participation

Social media presents several unique risks. Specifically, we will detail how social networks aid information revelation and thus aid phishing attacks, lead to regretful social media posts, and to aids corporate espionage.

4.1 *Increased Information Revelation*

Information disclosure is a well-documented issue in social networking sites. Wilcox and Stephen [34] found that a five minute session on Facebook could reduce self control. And as pointed out by Acquisti and Gross [1], individuals often believe themselves to be releasing far less information than they are. Furthermore, once information is inappropriately shared; individuals can experience regret but they cannot undo the disclosure [32]. One way to view the issue of social media regrets is as an interface failing - users who accidentally reveal personal information simply did not understand the privacy control interface. However, research shows that this logic is flawed. For example, Stutzman et al. [31] found that while Facebook users increasingly take advantage of privacy controls to limit what they share with the entire internet, and that the amount of information shared privately to other Facebook users actually increased. This finding corroborates Brandimarte et al.'s work [9], which found that the more control users were given over publication of personal information, the less users exhibited privacy concerns, even if the probability that a stranger was the same with or without the privacy controls. Taken together, these studies show that users seek a sense of control, and that when given privacy controls, users will feel comfortable and share more information regardless of if these privacy controls are effective. This is in line with other risks, on and off line, where the ability to mitigate a risk makes the risk more acceptable [2, 18]. In addition to the obvious issues with oversharing (e.g., a

post is viewed by an unintended party), structural properties of social networks can exacerbate the harm caused by regretful posts [8]. Camp and Chien first discussed the structural implications the internet as a public space [10], and how traditional notions of what is private and public could be affected by the dynamics of the internet. Approximately a decade later, after the rise of social networking, danah boyd would confirm Camp and Chein's fears, detailing [8] how networked publics such as social networking sites (SNS) are a new type of space. Boyd illustrated how SNS structures have unique privacy implications, specific to their electronic nature. boyd elaborated on four specific structural properties of SNSs that have privacy implication,

1. *Persistence*" - the idea that SNS posts can (and often are) permanently archived.
2. *Scalability*" - the potential visibility of any given SNS post is mostly dependent on the size of the social network.
3. *Replicability*" - it is trivial to duplicate SNS posts
4. *Searchability*" - the content in these networked publics can easily be found through search.

In addition to the above properties, most social networking posts lack what Nissenbaum [25] has termed "contextual integrity". Contextual integrity is integral to privacy. The concept of contextual integrity rejects a dichotomy between public and private life, and instead instead says that information is contextual. For example, a bar is "public", and a person may not mind if other people in a bar see their behavior at said bar. But these patrons probably would not want their actions broadcast to coworkers or family members. Simply put, the properties of networked publics make posts on easy to find and easier to spread once found. Users may make posts which in one context (such as among friends) are perfectly acceptable, but in another context (such as a conversation with a business recruiter) may be inappropriate. On social networking sites, contextual integrity is seldom. The default setting on many social networking sites (e.g., Twitter, Facebook) are that updates go out to one's entire social circle (or sometimes the public at large), regardless of context. A snapshot from a night out at the bar with friends after a hard day's work might be innocent and fun when shared with close friends, but serve as career limiting information when shared with upper management. When social networking sites change their terms of service, it often raises the ire of privacy advocates. Sometimes, users themselves become frustrated when they regret revealing career limiting information due to confusing privacy controls [32]. These revelations can have severe consequences. For example, in the United States, there are a set of protected classes of data based on histories of discrimination. Discrimination based on race, color, religion, national origin, age, sex, pregnancy, citizenship, familial status, disability status, veteran status, or genetic information is prohibited under US federal law. Yet many of these variables (often excluding disability) is either transparently easy to observer or included as part of the "basic information" in a Facebook profile. Other traditionally "private" data, such as political affiliation and sexual orientation, are also often observable from SNS data [22]. State laws may further prohibit discrimination on sexual orientation; another data component often communicated in SNS disclosures. In cases where information is *not* related to a protected class, then an employer is free to terminate an employee based on this information — even if said behavior does not violate any local or federal laws. "Facebook fired" is an emerging slang phrase describing those situations where posts on social networking result in loss of employment. For example, in August 2009 a 24 year old high school teacher in Georgia was forced to resign after posting a picture of herself apparently holding an alcoholic beverage was posted to Facebook [24]. As of this writing, participation on SNSs is not mandatory. The argument can be made that if a user is dissatisfied with a TOS change or a privacy interface they can simply leave the service. However, leaving a social network does not remove all risk. For example, Facebook was cited by the FTC for retaining data users had deleted, and has previously revealed information that users had restricted via their privacy settings [13]. And information once posted can be crawled and archived. Thus, deleting a post on a social network evoke's Whitten et al's [33] "barn door property": information once released cannot be reliably recalled.

4.2 *Providing "Open Source" Intelligence*

Governments are increasingly relying on so called "open source" intelligence[5] to aid operations. Attackers can use social media to launch other social engineering attacks, to identify physical locations to burglarize, and otherwise utilize what the military terms "open source intelligence" in order to craft more believable social engineering and phishing attacks, by utilizing information that a user mistakenly believes only known to a close peer.

Participation in SNS provides information to criminals as well as colleagues. Appeals for financial authenticating authenticating information or direct monetary transfer may be more effective if personalized. Phishing (attempting to gain authenticating information by masquerading as a trusted entity) is increasing. $687M was lost to masquerade attacks in 2012 alone; a 32% increase over 2011 [30]. Highly customized "spear phishing" has also increased. While typical phishing messages are sent out *en masse*, spammed to hundreds of thousands of peo-

ple, a spear phishing message is only sent to one person. Spear phishing messages utilize details from the target's life to make their message more realistic. For example, a spear phisher may forge their email header to appear to be a target's supervisor. Using social networks can increase your risk of being spear phished. For example, Ryan et al. [29] created a fake persona named "Robin Sage", who falsely claimed to be an attractive female cyber threat analyst for the Naval Network Command Center. Within weeks, Robin had social network connections with hundreds of defense industry professionals. Specifically, connections that could be valuable in gathering information for social engineering attacks. These include spear phishing attacks — social engineering attacks which attempt convince a target to launch a malware-ridden attachment.

5 Conclusions

As we have seen above, social networking cites can lead to the over sharing of personal information. However, abstention from social networking sites has a very real economic cost, by limiting networking opportunities. Furthermore, abstaining from social networking can increase one's risk of impersonation and cause one to be perceived as untrustworthy. Additionally, abstention can lead to higher prices, since abstaining users lack the social signal used by many entities to determine hiring. Abstaining from SNSs does not stop these SNSs from tracking the user. For example, a report commissioned by the Belgian data protection agency [4] found that Facebook tracked users who had opted out and who had not ever registered for Facebook. In conclusion, given that web tracking is inevitable whether a user registers for a SNS, that abstaining from SNSs carries risks such as impersonation and slander, and that there are significant economic harms sustained from abstaining from social networking, we conclude that a "rational actor" attempting to maximize one's salary and minimize harm would thus choose to use social networking. Thus, we can conclude that arguments that social networking users should accept the confusing privacy interfaces, frequent TOS changes, and other abuses present in many online social networks is deeply flawed. We propose instead that social networks embed privacy by design [11] to reduce information dissemination. This means designing social network interfaces from the ground up to enhance privacy, enabling strong privacy protections by default. For example, Stuzman et al. [31] showed a large jump in sharing by Facebook users as the result Facebook making "likes" public by default in 2011. Conversely, a SNS provider wishing to embed privacy by design would choose to make information private by default. We also recommend that private industry forms self regulatory guidelines on the use of social media data in hiring/firing decisions. For example, in the United States Federal Law protects job applicants from discrimination based on race, color, religion, national origin, age (40 and over), sex, familial status, disability status, veteran status, or genetic information. While it is technically legal for a company to request this information (just not legal to act on it), in the interest of avoiding any appearance of impropriety, many companies have implemented internal human resources policies not ask questions that would cause an applicant to reveal such information. As it currently stands, companies may be sidestepping policies against asking about protected class information under the guise of looking for "unprofessional behavior". As we have demonstrated, users seeking maximal economic gains and who wish to eliminate the many risks inherent in *not* maintaining a social networking profile must give up their privacy and join a SNS. Thus, since many companies acknowledge that asking for certain protected information is inappropriate and voluntarily choose not to collect said information, they should be equally willing to pledge not to plunder SNSs for that same information. Given that viewing an SNS page, unlike being asked about one's protected information in an interview, is not readily apparent to the user (and thus more rife for abuse), we propose that companies be legally barred from looking up the social networking profiles of job applicants.

Acknowledgments

Research was sponsored by the Army Research Laboratory under Cooperative Agreement Number W911NF-13-2-0045 (ARL Cyber Security CRA). This material is based upon work supported, in part, by the DHS BAA 11-02-TTA 03-0107 Contract N66001-12-C-0137, Cisco Research Support Proposal 591000 and Google Privacy & Security Focused Research Program. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the DHS, DoD, Google, Indiana University, or the Center for Democracy & Technology. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

Travel to the Amsterdam Privacy Conference was made possible by a generous $1000 USD grant from the Indiana University Center for Applied Cyber Security Research, as well as the Center for Democracy & Technology. The authors would further like to thank the various Center for Democracy & Technology staff members

whose feedback on early versions of this work served invaluable, including Joseph Lorenzo Hall, Alethea Lange, and Justin Brookman.

References

[1] ACQUISTI, A., AND GROSS, R. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers* (2006), vol. 4258, Springer-Verlag New York Incorporated, p. 36.

[2] ADAMS, J. *Risk*. Routledge, February 1995.

[3] AIRBNB. Why shoukd i connect to facebook?

[4] ALSENOY, B. V., VERDOODT, V., HEYMAN, R., AUSLOOS, J., WAUTERS, E., AND ACAR, G. From Social Media Service to Advertising Network: A Critical Analysis of Facebooks Revised Policies and Terms.

[5] ALSENOY, B. V., VERDOODT, V., HEYMAN, R., AUSLOOS, J., WAUTERS, E., AND ACAR, G. Spy Agencies Turn to Newspapers, NPR, and Wikipedia for Information.

[6] BEAMAN, L. Social Networks and the Dynamics of Labour Market Outcomes: Evidence from Refugees Resettled in the US. *The Review of Economic Studies 79*, 1 (2012), 128–161.

[7] BÖHME, R., KOBLE, S., AND DRESDEN, T. On the Viability of Privacy Enhancing Technologies in a Self Regulated Business to Consumer Market: Will Privacy Remain a Luxury Good. In *Workshop on the Economics of Information Security (WEIS), Carnegie Mellon University, Pittsburgh, PA* (2007).

[8] BOYD, D. Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In *Networked Self: Identity, Community, and Culture on Social Network Sites (ed. Zizi Papacharissi)* (2010), pp. 39–58.

[9] BRANDIMARTE, L., ACQUISTI, A., AND LOEWENSTEIN, G. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* (2012).

[10] CAMP, J., AND CHIEN, Y. The Internet as Public Space: Concepts, Issues, and Implications in Public Policy. *ACM SIGCAS Computers and Society 30*, 3 (2000), 13–19.

[11] CAVOUKIAN, A., TAYLOR, S., AND ABRAMS, M. E. Privacy by Design: Essential For Organizational Accountability and Strong Business Practices. *Identity in the Information Society 3*, 2 (2010), 405–413.

[12] CINGANO, F., AND ROSOLIA, A. People I Know: Job Search and Social Networks. *Journal of Labor Economics 30*, 2 (1999), 291–332.

[13] COMMISSION, F. T. In the Matter of Facebook, inc., a Corporation FTC File No. 092 3184, Aug. 2012.

[14] DIMAGGIO, P., AND GARIP, F. How Network Externalities Can Exacerbate Intergroup Inequality1. *American Journal of Sociology 116*, 6 (2011), 1887–1933.

[15] FINN, P. Lanzas Brrother Denies Giving Facebook Interview to New York Post, Dec. 2012.

[16] FISHER, C. S. *America Calling: Social History of the Telephone to 1940*. Univ of California Press, 1992.

[17] FRIEDMAN, E. J., AND RESNICK, P. The Social Cost of Cheap Pseudonyms. *Journal of Economics and Management Strategy* (2001).

[18] GARG, V., AND CAMP, J. Heuristics and Biases: Implications for Security Design. *Technology and Society Magazine, IEEE 32*, 1 (2013), 73–79.

[19] GRANOVETTER, M. S. The Strength of Weak Ties. *American journal of sociology* (1973), 1360–1380.

[20] HILL, K. Beware, Tech Abandoners: People Without Facebook Accounts Are 'Suspicious.', Aug. 2012.

[21] KLOUT. What is Klout?

[22] KOSINSKI, M., STILLWELL, D., AND GRAEPEL, T. Private Traits and Attributes are Predictable from Digital Records of Human Behavior. *Proceedings of the National Academy of Sciences* (2013).

[23] LEVIN, D., WALTER, J., AND MURNIGHAN, J. Dormant Ties: The Value of Reconnecting. *Organization Science 22*, 4 (2011), 923–939.

[24] NEWS, G. D. Teacher Ashley payne fired for posting picture of herself holding beer on facebook.

[25] NISSENBAUM, H. Toward an Approach to Privacy in Public: Challenges of Information echnology. *Ethics & Behavior 7*, 3 (1997), 207–219.

[26] NORCIE, G., DE CRISTOFARO, E., AND BELLOTTI, V. Bootstrapping trust in online dating: Social verification of online dating profiles. In *Financial Cryptography and Data Security*. Springer, 2013, pp. 149–163.

[27] ODLYZKO, A. Privacy, Economics and Price Discrimination on the Internet. In *Economics of Information Security* (New York, NY, 2004), L. J. Camp and S. Lewis, Eds., vol. 12 of *Advances in Information Security*, Springer, pp. 187–212.

[28] POPPER, B. Your Klout Score Must Be Greater Than 35 To Read This Post.

[29] RYAN, T., AND MAUCH, G. Getting in Bed with Robin Sage. In *Black Hat Conference* (2010).

[30] SOFTPEDIA. RSA: Phishing Attacks Worldwide Cause Losses of $687m (556m) in h1 2012, Aug. 2012.

[31] STUTZMAN, F., GROSS, R., AND ACQUISTI, A. Silent listeners: The evolution of privacy and disclosure on facebook. *Journal of Privacy and Confidentiality 4*, 2 (2013), 2.

[32] WANG, Y., NORCIE, G., KOMANDURI, S., ACQUISTI, A., LEON, P. G., AND CRANOR, L. F. "i regretted the minute i pressed share": A Qualitative Study of Regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (2011), ACM, p. 10.

[33] WHITTEN, A., AND TYGAR, J. D. Why johnny cant encrypt: A usability evaluation of pgp 5.0. In *Proceedings of the 8th USENIX Security Symposium* (1999), vol. 99, McGraw-Hill.

[34] WILCOX, K., AND STEPHEN, A. Are Close Friends the enemy? Online Social Networks, Self-Esteem, and Self-control. *Journal of Consumer Research, Forthcoming* (2012), 12–57.

[35] WISNIEWSKI, P., XU, H., LIPFORD, H., AND BELLO-OGUNU, E. Facebook Apps and Tagging: The Trade-Off Between Personal Privacy and Engaging with Friends. *Journal of the Association for Information Science and Technology* (2015).