Forget Me Do^{TM}: Empowering user privacy on social network sites

Ben Smyth

Forget Me Do^{TM} Limited Technical Report 2014/10
October 16, 2014

Document history

Version	Date	Comment
0.1	16 October 2014	Internal release
0.2	6 December 2015	Press release
0.3	17 December 2015	Public release

Forget Me Do™: Empowering user privacy on social network sites

Ben Smyth

October 16, 2014

Abstract

Social network sites support identity, relationships, and community. These three attributes of social interaction are fundamental to the basic human need for love, affection, and belongingness; creating a powerful motivation for the adoption of social network sites. By definition, social interaction cannot be conducted in private and social network sites have resulted in an unprecedented deluge of information revelations.

Information revelations on social network sites expose individuals to the risk of privacy violations. Facts unearthed by these violations have the potential to crush the basic human need for love, affection, and belongingness. We respond to the risks associated with information revelations: we propose deleting information that can be used to an individual's disadvantage. Thereby freeing individuals from the consequences of information revelations. We acknowledge that deleting all information is not a viable solution, since this would eliminate the advantages offered by social network sites. We overcome this issue by only deleting information that satisfies some deletion criteria. For instance, information older than a particular date.

We have implemented our response as a smartphone application called Forget Me Do™, which automatically deletes status updates and removes tags from photos stored on Facebook®. The app is available on Android® and iOS™. We hope to extend our app to other social network sites in the future. Our response does not rely on software modifications to social network sites, hence, we immediately empower the general public with a tool that mitigates against the harms posed by information revelations.

1 Social network sites

Social network sites are "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system" [bE07]. This definition embodies three attributes of social interaction that social network sites support [Gri08]:

- *Identity*: individuals create profiles that represent them.
- *Relationships*: individuals establish one-to-one connections with others.
- *Community*: individuals occupy a specific place among their peers.

These attributes of social interaction are fundamental to the basic human need for love, affection, and belongingness. Maslow [Mas43] argues that this basic need dominates consciousness, once physiological and safety needs are satisfied, thereby creating a powerful motivation for the adoption of social network sites.

Profiles are a core feature of social network sites. They allow individuals to reveal a representation of themselves. This can be achieved by disclosing personal information, including: name, age, gender, home town, contact information, education and employment histories, sexual preference, religious beliefs, and political views. Moreover, thoughts and feelings can be expressed by ephemeral status updates, and experiences can be shared using multimedia content such as photos and videos. Profiles also facilitate relationships. For example, statuses and multimedia content support comments and tags, and messages can be posted to an individual's profile. By definition, profiles reveal information.

Information revelation. The social network site Facebook® boasts 829 million daily active users [Fac14, pp1]. Every day, these users upload more than 4.75 billion items of content (including status updates, wall posts, photos, videos, and comments), 'like' more than 4.5 billion items, and send more than 10 billion messages [FEQ13, pp6], contributing to the 600 terabytes of data collected by Facebook® every day [VW14]. This unprecedented deluge of information revelation can be attributed to "the important, even primal, human desire [to] craft social identities, forge reciprocal relationships, and accumulate social capital" [Gri08].

The desire for social interaction cannot be conducted in private: "identity [revelations] require an audience; relationships are impossible without others; community *is* a public" [Gri08].

2 Consequences of information revelation

In terms of Solove's taxonomy of privacy [Sol06], social network sites expose individuals to privacy violations involving:

- *Aggregation*: the combination of various pieces of data about a person.
- *Disclosure*: the revelation of truthful information about a person that impacts the way others judge her character.[1]

[1] We include self-exposure [Sol07, pp196–200] – that is, personally revealing information about one's self – in the definition of disclosure.

- *Increased accessibility*: the amplification of information accessibility.
- *Insecurity*: the maladministration of stored information.
- *Second use*: the use of information collected for one purpose for a different purpose without the data subject's *explicit* consent.[2]
- *Surveillance*: the observation of an individual's activities.

Let us explore each of these issues in more detail:

Aggregation. Privacy violations involving aggregation exploit the fact that "a comprehensive collection of data about an individual is vastly more than the sum of its parts" [Coh00]. For instance, suppose a 23 year old female shopper from Atlanta buys the following items in March: cocoa-butter lotion, a handbag large enough to contain diapers, magnesium and zinc supplements, and a bright blue rug. Taken individually, each item is innocuous; however, the combination of items allows us to deduce that there is "an 87 percent chance that she's pregnant and that her delivery date is sometime in late August" [Duh12]. Unexpectedly, aggregation reveals sensitive facts from non-sensitive data.

Disclosure. Privacy violations involving disclosure arise when private concerns – including past mistakes and misconduct – are revealed [Sol03]. For instance, Swidey [Swi03] discusses the problems faced by a man who wrote about his teenage incarceration during the '90s and how he "never saw Google coming - how those tiny publications would go online and into the claws of the nation's top Internet search engine, and how a bored co-worker or prospective employer would be able to get up close and personal with [his] wild ride as a teenager." Although disclosure releases correct information, it may "thwart opportunities in one's future" [Sol07, pp49] and allowing individuals to hide these past indiscretions fosters change, without the burden of "a public transcript of consciousness" [Joh10].

Increased accessibility. Privacy violations involving increased accessibility occur when a norm of flow is violated, that is, when information is available beyond a boundary dictated by common practice [Nis04]. For instance, the norm of flow for profiles dictates that information must be requested. Facebook® violated this norm of flow with the introduction of its 'News Feed' feature, which broadcasts information from profiles, thereby breaching the requirement that profile information must be requested. Despite the availability of information by diligent search, increased accessibility causes "the sense of exposure and invasion" [boy08].

[2] We broaden Solove's definition of second use to include cases where the data subject gives *implicit* consent.

Insecurity. Privacy violations involving insecurity exploit carelessness in protecting stored information from leaks and improper access. For instance, insufficient encryption has resulted in session hijacking [But10, Mar10], inefficient anonymisation has enabled tracking of individuals [KW10], and insufficient authentication has permitted unauthorised access to information [Lie08, Clu11, Clu12, Duc13, Duc14]. Insecurity exposes information that should be private.

Second use. Privacy violations involving second use arise when information is used beyond the scope for which it was collected. For instance, Facebook® has carefully crafted an agreement which permits amendments to information usage by implicit consent: using Facebook® after amendments have been made constitutes acceptance of the amended terms [Fac13, §14]. (Cf. "[Facebook® has] slowly but surely helped itself – and its advertising and business partners – to more and more of its users' information" [Ops10] and McKeon's graphical representation of the problem [McK10].) Secondary use essentially denies individuals the right to control future uses of their information.

Surveillance. Privacy violations involving surveillance occur when the social norm of civil inattention [Gof71] – or, more directly, the social norm against snooping [Gri08, §2.3.2] – is violated. For instance, "people with no social connection to you *could* look at your profile but *shouldn't*" [Gri08, §2.3.2]. It follows that surveillance includes discovery by legal professionals [Min08], background checks by employers [Sol07, pp38], and searches by private investigators [Ahe10, §3 & §12]. Although surveillance unveils public information, there is an expectation of civil inattention and violations cause self-censorship [Kan98, §3.1.2] and inhibition [Swi99, §1.3.2].

Love, affection and belongingness – basic human needs that have driven many to adopt social network sites – have the potential to be crushed by facts unearthed by privacy violations; protecting our fundamental needs is of utmost importance.

3 Responses (that don't work)

Based upon Goffman [Gof59], Grimmelmann [Gri08, §3] and Mayer-Schönberger [May11, §5], we recall the following responses:

- *Abstinence*: information revelations can stop.
- *Cognitive adjustment*: evolution will enable humans to cope.
- *Expiry dates*: data can be deleted on a pre-defined expiry date.
- *Impression management*: damaging information can be removed.
- *Legislation*: legal frameworks can restrict the flow of information.
- *Market forces*: economics will naturally ensure the right degree of privacy.

Unfortunately, none of these responses offer sufficient protection against information revelation:

Abstinence. Abstinence assumes individuals will stop using social network sites once the consequences have been understood. The argument is dependent upon the consequences of usage outweighing the benefits that such sites offer; this seems unlikely. Moreover, abstinence does not counter the risk posed by information that has already been revealed.

Cognitive adjustment. Cognitive adjustment assumes the human race can adapt to cope with information revelations. For instance, Togelius [Tog07] remarks that isolated instances of disclosure in one's past "should not in any way be held against [one] when they later in life want to become a politician, teacher, babysitter, policeman etc. We will simply have to assume that people can change and restrict ourselves to looking at their most recent behaviour and opinions." The cognitive adjustment argument may be true, but evolution does not solve the problem of how humans will cope today.[3]

Expiry dates. Expiry dates assume that individuals will associate each piece of data with an expiry date and software (e.g., software maintained by social network sites) will delete data upon expiry. The notion necessitates software modifications, hence, expiry dates are dependent upon market forces (i.e., if individuals negotiate for expiry dates, then software providers will rationally respond by supplying them) and, thus, inherit problems associated with market forces (see below). Moreover, Mayer-Schönberger [May11, pp174] acknowledges that legislation, with its inherent problems (see below), is likely to be required to ensure that data is deleted. Furthermore, inputting expiry dates is likely to spoil the user-experience and places a cognitive burden upon individuals. Finally, the risk posed by information that has already been revealed is not addressed.

Impression management. Impression management assumes we can identify and remove damaging information. Unfortunately, these assumptions are plagued by economic problems: the cost of manually identifying and removing damaging information is expensive. For instance, based upon the figures in Section 1, an average Facebook® user uploads approximately 8500 pieces of information every year, which would take almost two days to identify and delete, assuming it takes 5 seconds to identify and remove each piece of information. In addition, the ability to identify damaging information suffers from: cognitive problems [Sol13, §1.1.2], for instance, "[individuals] will often be overwhelmed with the task of identifying possible outcomes related to privacy threats and

[3] We reject claims by Facebook®'s founder Mark Zuckerberg and Google chairman Eric Schmidt that humans have already adapted; we concur with boyd [boy14, pp56]: such claims are made "in order to justify their own business decisions regarding user privacy."

means of protection" [AG07, §18.3.1], and structural problems, for instance, "aggregation [...] makes it nearly impossible to manage data" [Sol13, §1.2.2].

Legislation. Legislation *can* restrict the flow of information. For instance, information deletion mandates can regulate how long information may be stored and privacy rights can empower individuals with control over their information. However, information deletion mandates assign the decision of what must be deleted, and when, to lawmakers, rather individuals [May11, pp160]. And, privacy rights are "difficult to enact, of dubious effectiveness, and [provide] no insurance against an uncertain future [and] the overall suitability of [privacy rights] is unclear" [May11, pp141]. Moreover, to avoid becoming too authoritarian, "[legislation] should be less involved when people are merely self-disclosing personal information" [Sol07, pp196], which limits protection against disclosure.

Market forces. Market forces assume that individuals will negotiate for privacy and social network sites will rationally respond by supplying it. The argument is dependent upon individuals understanding how much privacy they truly desire; unfortunately, evidence suggests that this precondition is false [Gri08, §3.1].

These responses provide insufficient protection against information revelation. Nonetheless, our response is inspired by expiry dates and impression management.

4 Our response: Forget Me Do™

To address the challenges posed by information revelation, we tackle the root of all privacy violations: the existence of information that can be used to an individual's disadvantage. We posit that deleting this information will free individuals from the consequences of information revelation. We accept that deleting all information is not a viable solution, since this would eliminate the benefits offered by social network sites. We overcome this issue by only deleting information that satisfies some deletion criteria. For instance, information older than a particular date.

Our response eliminates the cognitive problems associated with identifying damaging information (default deletion criteria can be predefined by experts, so this is not a cognitive issue). Moreover, criteria can be fine-tuned to ensure the right degree of privacy for each individual. Our response also minimises the structural problems associated with aggregation, since aggregation is less profitable when the available information is limited. In addition, economic costs can be eliminated by automation. We have implemented our response as a smartphone application.

Forget Me Do™ app. Our *Forget Me Do*™ smartphone application automatically deletes status updates and removes tags from photos stored on

Facebook®. The app is available on Android®[4] and iOS™[5]. We hope to extend our app to other social network sites in the future.

By implementing our response as a smartphone application, we empower individuals with a tool that combats the consequences of information revelation. The tool does not rely on software modifications to social network sites, hence, we avoid the dependencies on legislation and market forces that are typical of expiry dates.

5 Conclusion

Information revelations on social network sites expose us to the risk of privacy violations that may ruin individuals; appropriate responses to the risk are essential. We mitigate against the harms posed by information revelations: we propose deleting all information that satisfies some deletion criteria. For example, information older than a particular date. We have implemented our response as a smartphone application that automatically deletes status updates and removes tags from photos stored on Facebook®.

Our response is inspired by expiry dates, which teach us to define a deletion date for each piece of data that we reveal (and rely on the recipient to delete data upon expiry), and impression management, which teaches us to identify and remove damaging information. We improve upon expiry dates by eliminating the reliance on recipients deleting data and by defining some global deletion criteria, rather than associating each piece of data with some criteria. And we improve upon impression management by eliminating the need to consider whether information is damaging. Moreover, we eliminate economic costs through automation.

Our immediate objective is to empower the general public with tools that eliminate the consequences of information revelation. Longer-term, we want to stimulate debate on privacy and, ultimately, help revolutionise society's perspective of privacy.

References

[AG07] Alessandro Acquisti and Jens Grossklags. What Can Behavioral Economics Teach Us About Privacy? In Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis, and Costas Lambrinoudakis, editors, *Digital Privacy: Theory, Technologies and Practices*, chapter 18. Auerbach Publications, 2007.

[Ahe10] Frank M Ahearn. *How to Disappear: Erase Your Digital Footprint, Leave False Trails, And Vanish Without A Trace*. Lyons Press, 2010.

[4] `https://forgetmedo.com/android-app`
[5] `https://forgetmedo.com/ios-app`

[bE07] danah boyd and Nicole Ellison. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), 2007.

[boy08] danah boyd. Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence. *Convergence: International Journal of Research into New Media Technologies*, 14(1), 2008.

[boy14] danah boyd. *It's Complicated: The Social Lives of Networked Teens*. Yale University Press, 2014.

[But10] Eric Butler. Firesheep, October 2010. http://web.archive.org/web/20101026141114/http://codebutler.com/firesheep.

[Clu11] Graham Cluley. Facebook fixes flaw that allowed access to private photos, December 2011. http://web.archive.org/web/20120107154836/http://nakedsecurity.sophos.com/2011/12/07/facebook-fixes-flaw-that-allowed-access-to-private-photos/.

[Clu12] Graham Cluley. Hacker exposes Grindr users' intimate information and explicit photos, January 2012. http://web.archive.org/web/20120122230220/http://nakedsecurity.sophos.com/2012/01/20/grindr-hack/.

[Coh00] Julie E Cohen. Examined lives: Informational privacy and the subject as object. *Stanford Law Review*, 2000.

[Duc13] Paul Ducklin. Facebook issues data breach notification - may have leaked your email and phone number, June 2013. http://web.archive.org/web/20130826030426/http://nakedsecurity.sophos.com/2013/06/23/facebook-issues-data-breach-notification-may-have-leaked-your-email-and-phone-number/.

[Duc14] Paul Ducklin. Attack dismissed as "theoretical" by Snapchat used to plunder 4.6 million phone numbers, January 2014. http://web.archive.org/web/20140125104229/http://nakedsecurity.sophos.com/2014/01/01/attack-dismissed-as-theoretical-by-snapchat-used-to-plunder-4-6-million-phone-numbers/ See also http://web.archive.org/web/20140101042651/http://www.snapchatdb.info/.

[Duh12] Charles Duhigg. How Companies Learn Your Secrets. New York Times, February 2012. http://web.archive.org/web/20120216174029/http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[Fac13] Facebook®. Statement of Rights and Responsibilities, November 2013. https://www.facebook.com/legal/terms and https://web.archive.org/web/20141002025013/https://www.facebook.com/legal/terms.

[Fac14] Facebook®. Facebook Reports Second Quarter 2014 Results, 2014. https://web.archive.org/web/http://files.shareholder.com/downloads/AMDA-NJ5DZ/0x0x770574/0559fb66-5557-4ced-ba22-c0a1579e7c31/FB_News_2014_7_23_Financial_Releases.pdf.

[FEQ13] Facebook®, Ericsson®, and Qualcomm®. A focus on efficiency, September 2013. http://internet.org/efficiencypaper, https://web.archive.org/web/20130916203056/http://internet.org/efficiencypaper, and http://web.archive.org/web/20140530041730/http://newsroom.fb.com/news/2013/09/focusing-on-efficiency/.

[Gof59] Erving Goffman. *The Presentation of Self in Everyday Life*. Anchor, 1959.

[Gof71] Erving Goffman. *Relations in Public*. Basic Books, 1971.

[Gri08] James Grimmelmann. Saving Facebook. *Iowa Law Review*, 94, 2008.

[Joh10] John D. Sutter. The internet and the 'end of privacy', December 2010. http://web.archive.org/web/20101216073558/http://edition.cnn.com/2010/TECH/web/12/13/end.of.privacy.intro/.

[Kan98] Jerry Kang. Information Privacy in Cyberspace Transactions. *Stanford Law Review*, 1998.

[KW10] Balachander Krishnamurthy and Craig E. Wills. On the leakage of personally identifiable information via online social networks. *Computer Communication Review*, 40(1), 2010.

[Lie08] Michael Liedtke. Security lapse exposes Facebook photos, March 2008. http://www.nbcnews.com/id/23785561/ns/technology_and_science-security/t/security-lapse-exposes-facebook-photos/.

[Mar10] Matt Markovich. Firesheep developer: Facebook ignoring huge security problem, November 2010. http://www.komonews.com/news/tech/107360348.html.

[Mas43] Abraham Harold Maslow. A theory of human motivation. *Psychological Review*, 50(4), 1943.

[May11] Viktor Mayer-Schönberger. *Delete: the virtue of forgetting in the digital age*. Princeton University Press, 4 edition, 2011.

[McK10] Matt McKeon. The Evolution of Privacy on Facebook, May 2010. http://web.archive.org/web/20100509051202/http://mattmckeon.com/facebook-privacy/.

[Min08] Kathrine Minotti. Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession, The. *South Carolina Law Review*, 60, 2008.

[Nis04] Helen Nissenbaum. Privacy as contextual integrity. *Washington Law Review*, 79, 2004.

[Ops10] Kurt Opsahl. Facebook's Eroding Privacy Policy: A Timeline, April 2010. http://web.archive.org/web/20100501032349/http://www.eff.org/deeplinks/2010/04/facebook-timeline.

[Sol03] Daniel J Solove. The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure. *Duke Law Journal*, 53(967), 2003.

[Sol06] Daniel J Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 2006.

[Sol07] Daniel J Solove. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale University Press, 2007.

[Sol13] Daniel J Solove. Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126(7), 2013.

[Swi99] Peter P Swire. Financial Privacy and the Theory of High-Tech Government Surveillance. *Washington University Law Review*, 77(2), 1999.

[Swi03] Neil Swidey. A nation of voyeurs: How the Internet search engine Google is changing what we can find out about one another – and raising question about whether we should. Boston Globe, February 2003. https://secure.pqarchiver.com/boston-sub/doc/405509756.html and https://secure.pqarchiver.com/boston-sub/doc/405504629.html.

[Tog07] Julian Togelius. Harvard Prof Says Computers Need to Forget: I disagree, May 2007. http://yro.slashdot.org/comments.pl?sid=234167&cid=19065957.

[VW14] Pamela Vagata and Kevin Wilfong. Scaling the Facebook data warehouse to 300 PB, April 2014. http://web.archive.org/web/20140411013927/https://code.facebook.com/posts/229861827208629/scaling-the-facebook-data-warehouse-to-300-pb/.