JICLT
Journal of International Commercial Law and Technology
Vol. 8, No.2 (2013)

Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services

Omer Tene[1]

"The biggest reason [I avoided joining Facebook] was that I didn't know which me would join. Apparently, Mark Zuckerberg believes we should all be the same in every context. According to Time's 2010 Person of the Year profile of him, he once told a journalist, 'Having two identities for yourself is an example of a lack of integrity.' To which my only response is, You've got to be kidding. I mean, I'm not even the same person with all the members of my immediate family. And I've long thought that my impulse to act differently with, say, my friend from grad school and my husband's aunt — to adjust my personality to fit the situation and the other person — is an example of good manners, not bad ones."[2]

1. Introduction

The Internet is used by more than 2 billion people worldwide for purposes ranging from electronic commerce, online banking, social networking, the consumption of media and the provision of electronic government services.[3] However, the Internet was not built with an embedded security and privacy infrastructure;[4] it lacks a system of identification[5] and authentication.[6] Typically, identity[7] is managed one application at a time.[8] This means that individuals are asked to maintain dozens of different usernames and passwords, one pair for each website with which they interact. The complexity of this approach is a burden to both individuals, who are driven to reuse passwords or utilize trivial ones such as relatives' birthdates, making online fraud and identity theft easier; and businesses, which are required to manage the identity of users despite not having the resources or interest to do so.[9] The Obama Administration's recent

---

[1] Associate Professor, College of Management Haim Striks School of Law, Israel; Affiliate Scholar, Stanford Center for Internet and Society; Fellow, Center for Democracy and Technology. I would like to thank the College of Management Haim Striks School of Law research fund and the College of Management Academic Studies research grant for supporting research for this article. I would also like to thank the participants in the Institute for Prospective Technological Studies Workshop on "Electronic Identity for Europe" for their helpful comments.

[2] Curtis Sittenfeld, I'm on Facebook. It's Over, NY Times Op Ed, September 3, 2011, http://www.nytimes.com/2011/09/04/opinion/sunday/if-im-on-facebook-it-must-be-over.html?_r=2.

[3] Internet Usage Statistics, Internet World Stats, http://www.internetworldstats.com/stats.htm.

[4] Jonathan Zittrain, The Future of the Internet and How to Stop It 31-33 (2008).

[5] Identification is the process of evaluating – based on the data provided – who a given person is; it is the association of data with a particular human being. *See* John Palfrey & Urs Gasser, Digital Identity Interoperability and eInnovation, Berkman Publication Series (2007).

[6] Authentication is the process of verifying the claimed identity of a user, process, or device. Ibid.

[7] An identity is "any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons. So usually there is no such thing as 'the identity', but several of them". Marit Hansen & Hannes Tschofenig, Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, IETF Working Document, March 14, 2011, http://tools.ietf.org/html/draft-hansen-privacy-terminology. An identity of an individual person may comprise many partial identities of which each represents the person in a specific context or role. *See generally* Roger Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues, 7,4 Information Technology & People 6-37 (December 1994).

[8] Identity management means "managing various identities (usually denoted by pseudonyms) of an individual person, i.e., administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role." Ibid.

[9] Joseph Smarr, Plaxo, Google I/O 2008: OpenSocial, OpenID, and OAuth: Oh, My! (June 9, 2008), http://www.youtube.com/watch?v=6SYnlH5FXz0, stating "every single site acts like you've never used another website before in your life."

National Strategy for Trusted Identities in Cyberspace (NSTIC)[10] emphasizes the importance of allowing people to choose among multiple identity providers, including not only government entities but also private businesses, to issue trusted credentials that prove identity. This goal is based on the realization that digital identities are used extensively not only in contexts requiring strong authentication, such as electronic voting or banking, but also for participating in online games, commenting on blog posts, or accessing music profiles. In Europe too, policymakers realize that electronic signatures, formal identities and public sector applications constitute only a part of a larger identity ecosystem for which there is no existing regulatory framework.[11] Increasingly, new focal points for the provision of identity services are emerging at the Internet's application layer. These are primarily social networking services (SNS), such as Facebook or Google Plus (which allows users to log in with their Gmail credentials), which benefit from extensive membership and are seeking to branch out into the open web.[12]

Indeed, Simson Garfinkel recently declared that "Facebook is in the process of transforming itself from the world's most popular social-media website into a critical part of the Internet's identity infrastructure."[13] He explains that Facebook is well suited to being the repository for people's identities on the Internet. Unlike many popular websites, it not only requires users to register and log in but also to "provide their real names and information."[14] Indeed, Facebook has terminated accounts that were created with seemingly fake names or for fictional characters.[15] Moreover, since Facebook users invest their accounts with a tremendous amount of durable personal content—including photographs, contact information, and connections to their social network—they are likely to keep a long-term relationship with the site. One of the most lucrative prospects for monetization by SNS operators of their role as purveyors of digital identity is the market for online and mobile payments. If SNS operators succeed in positioning themselves as providers or verifiers of digital identity for the purpose of processing payments, they stand to gain a cut of the entire market for e-commerce, which may be orders of magnitude greater than their current advertising revenues.[16]

In this article I explore some of the legal issues arising from the transformation of SNS operators to providers of digital identity. I consider the implications of the involvement of private sector entities in the field of identity management and discuss some of the privacy implications, as well as the prospects for conciliation between online anonymity and pseudonymity, on the one hand, and the need for identifiability and accountability on the other hand.

---

[10] National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[11] Anssi Hoikkanen, Margherita Bacigalupo, Ramón Compañó, Wainer Lusoli & Ioannis Maghiros, New Challenges and Possible Policy Options for the Regulation of Electronic Identity, 5(1) J. Int'l Commercial L. & Tech. 1 (2010), http://www.jiclt.com/index.php/jiclt/article/view/95/94; Wainer Lusoli, Ioannis Maghiros & Margherita Bacigalupo, eID policy in a turbulent environment: is there a need for a new regulatory framework?, European Commission Joint Research Centre (2009), http://www.epractice.eu/files/eID%20policy%20in%20a%20turbulent%20environment.pdf.

[12] Daniel Kahn, Social Intermediaries: Creating a More Responsible Web Through Portable Identity, Cross-Web Reputation, and Code-Backed Norms, 11 Colum. Sci. & Tech. L. Rev. 176 (2010).

[13] Simson Garfinkel, Facebook Wants to Supply Your Internet Driver's License, Technology Review, January 5, 2011, http://www.technologyreview.com/web/27027/page1/?a=f; *also see* Natasha Singer, Call It Your Online Driver's License, NY Times, September 17, 2011, http://www.nytimes.com/2011/09/18/business/online-id-verification-plan-carries-risks.html.

[14] Facebook, Statement of Rights and Responsibilities, Date of Last Revision: April 26, 2011, http://www.facebook.com/terms.php.

[15] The New York Times reported that Facebook recently de-activated an account used by world-acclaimed author Salman Rushdie, "demanded proof of identity and then turned him into Ahmed Rushdie, which is how he is identified on his passport. He had never used his first name, Ahmed, he pointed out; the world knows him as Salman." Somini Sengupta, Rushdie Runs Afoul of Web's Real-Name Police, NY Times, November 15, 2011, http://www.nytimes.com/2011/11/15/technology/hiding-or-using-your-name-online-and-who-decides.html?_r=1&hpw.

[16] *See* Launching Google Wallet on Sprint and working with Visa, American Express and Discover, The Official Google Blog, September 19, 2011, http://googleblog.blogspot.com/2011/09/launching-google-wallet-on-sprint-and.html; Jennifer Van Grove, Square Sets New Record: $2M Processed in One Day, Mashable, April 30, 2011, http://mashable.com/2011/04/29/square-payments.

2. Portability

In the context of SNS, data portability, and especially portable online identity, can mean two very different things. First, with data portability users are able to carry their online identity with them across different websites and services, using a uniform user-identification system, as opposed to re-establishing their identity on each site. Instead of online identities being segregated into single-site territories, users utilize a single set of credentials to log into multiple sites and services. I will call this type of portability "credentials portability".

Second, portable online identity may mean that users are allowed to migrate between platforms with their established identity without being locked-in by an existing SNS. Hence, if you have an account on MySpace which you have invested in for years, creating a network of friends, posting content and comments, uploading photos etc., you will be able to transfer the data in the account en masse to Facebook without having to reestablish your network and reinvent your identity. I will call this type of portability "data portability".

Both credentials portability and data portability have costs and benefits. Credentials portability, essentially the introduction of a uniform protocol for authenticating user identity, solves the awkwardness of having to create a new account for each and every online service. It improves data security, since users who need to memorize dozens of user names and passwords tend to either use the same password over and over again; adopt passwords that are overly simplistic and easy for rogue actors to attack; record their passwords elsewhere; or use the "forgot my password" feature offered by many sites, effectively staking those sites' data security on that of Gmail or another ubiquitous webmail services.

The flip side, of course, is that malicious attackers who obtain such a "master key" can now infiltrate more websites than one.[17] In a chilling illustration of these risks, hackers – ostensibly operated by the Iranian government – have recently infiltrated a Dutch certificate authority to issue forged Google certificates and used them to launch man-in-the-middle attacks against Gmail users and read their mail.[18] In its Interim Report analyzing the breach, security firm Fox-IT observes: "Not only the email itself, but also a login cookie could have been intercepted. Using this cookie the hacker is able to log in directly to the Gmail mailbox of the victim and also read the stored e-mails. Besides that, he is able to log in all other services Google offers to users like stored location information from Latitude or documents in Google Docs. Once the hacker is able to receive his targets' email he is also able to reset passwords of others services like Facebook and Twitter using the lost password button. The login cookie stays valid for a longer period. It would be wise for all users in Iran to at least logout and login but even better change passwords".[19] Clearly, leaving the keys to one's digital identity in the hands of a SNS operator is worrying.

Another benefit of credentials portability is that it allows individuals to participate in the "reputation economy", amalgamating their online presence to achieve cross-Web recognition.[20] It also enhances trust in the sense advocated by David Johnson, Susan Crawford and John Palfrey in their important essay "The

---

[17] SNS operators still rely on a single user name and password to gain access to an account. In the future, they could employ two factor authentication, requiring users to access their mobile phones to complete the log in process. Facebook already monitors a number of "signals," including location and device, to determine when an account is suspect of being subjected to attack. Simon Axten, a spokesperson for Facebook, tells Simson Garfinkel: "Once we've flagged an attempt—even if the correct login credentials have been entered—we'll require the person logging in to provide additional authentication by, for example, answering a security question, entering a code sent via SMS, or identifying friends tagged in photos to which the account owner has access." Garfinkel, *supra* note 13. *See generally*, Giles Hogben, Security issues in the future of social networking, ENISA Position Paper for W3C Workshop on the Future of Social Networking, September 2008, http://www.w3.org/2008/09/msnws/papers/Future_of_SN_Giles_Hogben_ENISA.pdf.

[18] Somini Sengupta, In Latest Breach, Hackers Impersonate Google to Snoop on Users in Iran, NY Times, August 30, 2011, http://www.nytimes.com/2011/08/31/technology/internet/hackers-impersonate-google-to-snoop-on-users-in-iran.html?_r=4.

[19] Fox-IT, DigiNotar Certificate Authority breach 'Operation Black Tulip', Interim Report, September 5, 2011, at p. 8, http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf.

[20] Kahn, *supra* note 12. Kahn points out that users can accrue cross-Web recognition even without a uniform identity using hyperlinks; *i.e.*, you might place links and cross-links to your page on different websites referring other users, for example, from your homepage to your blog, Facebook, Twitter, Google Plus profiles, SSRN page, etc. Yet, as Kahn points out "this ad hoc method of linking cross-site activity does not scale; it might work to cross-link activities on a handful of sites, but not on a hundred".

Accountable Internet".[21] Johnson, Crawford and Palfrey explain that new authentication, identification and authorization technologies will give users greater control over their digital connections so that online connections are established based on trust. They foresee an Internet where users are more accountable to one another than they have been in the past.

The past few years have seen a proliferation of uniform authentication standards, most notably Facebook's Open Graph (originally launched as Facebook Connect)[22] and Google's Friend Connect. Other projects include OpenID, an authentication service standard, which allows users to obtain a globally unique identity (a URL) which they can use anywhere, logging in to their OpenID provider instead of in to the sites that use OpenID; OAuth, which provides an authentication and authorization standard, allowing users to grant revocable, time- and scope-limited, third-party access capabilities to their account, instead of giving out their username and password which results in unrestricted access.

The main drawback of a single sign on authentication mechanism is the privacy problem that it creates.[23] Credentials portability essentially means putting your identity eggs in one basket. The multi-directional data flows established by the implementation of credentials portability are staggering. They include data flows from third party websites and applications to the service provider, typically a SNS operator, which becomes privy to not only a user's interaction with its service, but also with other websites that implement its user authentication platform. Hence, for example, a website participating in Facebook's Open Graph displays for users content that has been popular with their Facebook friends and allows them to share content they enjoy with others.[24] A key feature of Open Graph is that sites can add a "like" or "recommend" button; when users click the button, it adds a link to the site on their Facebook profiles; shares the link with their Facebook friends; and displays their names and photographs to Facebook friends who visit the site.[25] This functionality has recently been boosted by what Facebook calls "frictionless sharing";[26] the basic idea being that clicking a "Like" button is too burdensome so users can now authorize Facebook applications such as The Washington Post Social Reader or popular music streaming service Spotify to do the sharing for them with no additional action on their part.[27] Even if a user does not click on the Like button, Facebook gets to see where she is browsing, since the user is literally "browsing" to Facebook via the iFrame integrating social features into the third party site. In other words, if you are a Facebook subscriber, then whenever you open a page showing the "like" button, your visit is reported to Facebook; you do not have to click the button to trigger this report; nor is the information conveyed to Facebook anonymized; the report contains your Facebook identity information as well as the URL of the page you are looking at.[28] Indeed, a recent report alleged that Facebook monitors users' activity on third party websites even when they are not logged in to the system.[29]

---

[21] David Johnson, Susan Crawford & John Palfrey, The Accountable Internet: Peer Production of Internet Governance, 9 Va. J. L. & Tech. 9, 82 (2004).

[22] Facebook's Open Graph, also known as the Facebook Platform, provides more than just the user authentication service Facebook Connect. It stands for a stack of services allowing applications—websites, desktop, mobile, applets—to be written on top of the Facebook social network, providing authentication, authorization, and access to the social graph. For authentication using Facebook's platform *see* http://developers.facebook.com/docs/authentication.

[23] Garfinkel, *supra* note 13; Marit Hansen & Ari Schwartz, Privacy and Identity Management, 6(2) IEEE Security & Privacy 38 (2008); Dave Birch, Internet driver's license?, Digital Identity Blog, January 10, 2011, http://digitaldebateblogs.typepad.com/digital_identity/2011/01/internet-drivers-license.html.

[24] *See, e.g.*, Sara Inés Calderón, The New York Times Is Latest Newspaper to Tightly Integrate Facebook, Inside Facebook, September 1, 2010, http://www.insidefacebook.com/2010/09/01/new-york-times-facebook-login-social-plugins.

[25] For Facebook's explanation of the "like" button *see* http://developers.facebook.com/docs/reference/plugins/like.

[26] Ben Parr, Facebook Reveals Major Updates at F8 (Video), Mashable, September 22, 2011, http://mashable.com/2011/09/22/facebook-f8-live-video.

[27] Frictionless sharing is an opt in service. Users must initially authorize a website or application to share their information with Facebook. In addition, users can specify on Facebook who will see their third party activity (*e.g.*, only friends, the public). Richard MacManus, The Pros & Cons of Frictionless Sharing, ReadWriteWeb, September 28, 2011, http://www.readwriteweb.com/archives/frictionless_sharing_pros_cons.php.

[28] James Brown, Gov2.0 and Facebook 'Like' Buttons, The Other James Brown, December 7, 2010, http://blogs.msdn.com/b/james_brown/archive/2010/12/07/gov2-0-and-facebook-like-buttons.aspx.

[29] Nik Cubrilovic, Logging out of Facebook is not enough, Nik Cubrilovic Blog, September 25, 2011, http://nikcub.appspot.com/logging-out-of-facebook-is-not-enough; also see John Moe, Facebook is tracking you whether you're logged on, logged off, or not even a Facebook user, Marketplace Tech Report, September 27, 2011, http://marketplace.publicradio.org/display/web/2011/09/27/tech-report-facebook-is-tracking-you.

Facebook denied these charges and stated any monitoring was used strictly for "safety and protection".[30] However, further reports stated that Facebook did change its logged out cookie policy as a result of the public discussion.[31]

In the reverse direction, credentials portability provides websites and applications that participate in Open Graph with access to massive amounts of Facebook user data.[32] For example, users who sign in with their Facebook credentials to travel website Tripadvisor are prompted to authorize the transfer of the following information from Facebook to the site:

> "Access my basic information. Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.
>
> Send me email. TripAdvisor may email me directly at tene.omer@gmail.com·
>
> Access my data any time. TripAdvisor may access my data when I'm not using the application.
>
> Check-ins. TripAdvisor may read my check-ins and friends' check-ins.
>
> Access my profile information. Likes, Music, TV, Movies, Books, Quotes, Events, Hometown, Current City, Education History and Work History.
>
> Access information people share with me. Hometowns, Current Cities, Likes, Music, TV, Movies, Books, Quotes, Education History, Work History, Events, Photos and Videos."[33]

Many users who quickly click-through this notification in order to access the application may not be fully aware of the surprising amount of information shared by Facebook with this (randomly chosen) third party. It includes not only a user's email address; but also offline access to her Facebook data ("access my data any time") (*i.e.*, when she is not visiting or using Tripadvisor); location information ("check ins"); and information posted and generated on Facebook by her friends ("information people share with me"). All of this information then becomes subject to Tripadvisor's privacy policy, which authorizes the sharing of user data with third parties including third party vendors, business partners, referring websites, social media services, affiliated companies, law enforcement authorities, courts, and potential partners to corporate acquisitions.[34]

Privacy problems related to credentials portability are not unsolvable. To begin with, users may be making a conscious choice to share information and get recommendations from their friends in return for a share of their privacy. Indeed, privacy-ceding online and mobile applications such as SNS and location-

---

[30] ZDNet reported a Facebook spokesperson said: "Facebook does not track users across the web. Instead, we use cookies on social plugins to personalize content (*e.g.*, show you what your friends liked), to help maintain and improve what we do (*e.g.*, measure click-through rate), or for safety and security (*e.g.*, keeping underage kids from trying to signup with a different age). No information we receive when you see a social plugins is used to target ads, we delete or anonymize this information within 90 days, and we never sell your information. Specific to logged out cookies, they are used for safety and protection, including identifying spammers and phishers, detecting when somebody unauthorized is trying to access your account, helping you get back into your account if you get hacked, disabling registration for a under-age users who try to re-register with a different birthdate, powering account security features such as 2nd factor login approvals and notification, and identifying shared computers to discourage the use of 'keep me logged in'." Emil Protalinski, Facebook denies cookie tracking allegations, ZDNet, September 25, 2011, http://www.zdnet.com/blog/facebook/facebook-denies-cookie-tracking-allegations/4044.

[31] Emil Protalinski, Facebook fixes cookie behavior after logging out, ZDNet, September 27, 2011, http://www.zdnet.com/blog/facebook/facebook-fixes-cookie-behavior-after-logging-out/4120.

[32] University of Virginia researchers found that over 90% of third party applications on Facebook have unnecessary access to private data. Adrienne Felt & David Evans, Privacy Protection for Social Networking Platforms, Workshop on Web 2.0 Security and Privacy (W2SP) 2008, http://w2spconf.com/2008/papers/s3p1.pdf. *Also see* Emily Steel & Geoffrey Fowler, Facebook in Privacy Breach: Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds, Wall Street Journal, October 18, 2010, http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

[33] To see this list click "Sign in with Facebook" on the top of Tripadvisor's homepage, http://www.tripadvisor.com.

[34] *See* Tripadvisor Privacy Policy, "With whom we share your information", http://www.tripadvisor.com/pages/privacy.html.

based services are rapidly growing in popularity.[35] Furthermore, platforms are currently being developed to facilitate more limited information sharing between SNS operators and third party websites. OAuth, for example, provides an authentication and authorization tool,[36] allowing applications to indicate their permissions via a scope attribute, thus limiting the extent of information sharing.[37] In NSTIC, the Obama administration set forth as its goal to "use privacy-enhancing technology and policies to inhibit the ability of service providers to link an individual's transactions, thus ensuring that no one service provider can gain a complete picture of an individual's life in cyberspace. By default, only the minimum necessary information will be shared in a transaction. For example, the Identity Ecosystem will allow a consumer to provide her age during a transaction without also providing her birth date, name, address, or other identifying data."[38]

Data portability, meanwhile, provides a user with the explicit right to withdraw her own data from a SNS and transfer them, as far as is technically feasible, into another application or service, unhindered by the incumbent SNS operator. Google has recently been applauded for introducing a data portability feature, Google Takeout, in connection with the launch of Google Plus.[39] Google Takeout permits users of various Google products to export their contacts, Google Buzz feed, Picasa photo albums, Google profile and their "Stream" in a format readable by other SNS. Facebook, by contrast, allowed users to export only their photos and News Feed, and only as HTML files that can be saved locally on their computers. Facebook does not allow users to export their complete profile and friends' contact details, stating this would be a violation of those third parties' privacy.[40] Given Facebook's massive share of the SNS market, it is clear why Google pursues data portability more vigorously than its competitor.[41]

Facebook stated that it "recognizes the value to users of data portability and has recently introduced a tool to allow its users to download a copy of their personal data from the service. This is a technically complex challenge given the rapidly evolving pace of development of services such as Facebook and because of the need to respect privacy settings for data that may have been uploaded by multiple individuals."[42] Facebook's privacy concerns, while arguably self-serving and opportunistic, are not baseless. Absent standardization of policies, migrating an entire profile (or identity) from one SNS to

---

[35] One might get the impression that young people today simply do not care about privacy. Yet this would be a misconception. In fact, empirical research consistently proves the contrary. A recent Pew Report, shows young adults (aged 18-29) are more likely than older users to say they limit the amount of information available about them online. Mary Madden & Aaron Smith, Reputation Management Online: How people monitor and maintain their identity through search and social media, Pew Internet & American Life Project, May 26, 2010, http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx. Moreover, the Pew Report finds that among users of social networking sites, young adults are the most proactive in customizing their privacy settings and restricting who can see certain updates. Similar results have been reached by a group of Berkeley researchers, suggesting "that young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data." Chris Hoofnagle, Jennifer King, Su Li & Joseph Turow, How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?, April 14, 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.
For possible explanations of the apparent discrepancy between users' stated privacy preferences and their actions on SNS, *see* danah boyd, Making Sense of Privacy and Publicity, Keynote Address, SXSW, March 13, 2010, http://www.danah.org/papers/talks/2010/SXSW2010.html; Kate Raynes-Goldie, Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook, 15(1) First Monday (2010), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432.

[36] Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have to secured resources controlled by the system. *See* Steve Riley, It's Me, and Here's My Proof: Why Identity and Authentication Must Remain Distinct, Microsoft TechNet, February 14, 2006, http://technet.microsoft.com/en-us/library/cc512578.aspx.

[37] *Also see* Susan Landau, Hubert Le Van Gong & Robin Wilton, Achieving Privacy in a Federated Identity Management System, Financial Cryptography and Data Security (2009).

[38] NSTIC, supra note 10, at p. 2.

[39] Ryan Singel, Taking on Facebook, Google's Social Network Allows Data Exporting, Wired Epicenter, June 28, 2011, http://www.wired.com/epicenter/2011/06/google-facebook-export; Erick Schonfeld, Google Takeout, An Easier Way To Take Your Data With You, June 30, 2011, http://techcrunch.com/2011/06/30/google-takeout.

[40] *See, e.g.*, Stephen Shankland, Facebook blocks a second contact export tool, cnet, July 11, 2011, http://news.cnet.com/8301-30685_3-20078435-264/facebook-blocks-a-second-contact-export-tool/#ixzz1WvX7D79p.

[41] Declan McCullagh, Google wields data openness against Facebook, cnet, July 15, 2011, http://news.cnet.com/8301-31921_3-20079907-281/google-wields-data-openness-against-facebook.

[42] Facebook Response to European Commission Communication on personal data protection in the European Union, May 22, 2011, http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/facebook_en.pdf.

another may indeed result in mid-stream changes to privacy policies affecting third parties. James Grimmelmann expressed concern that data portability heightens the risk of divulging personal data which become subject to the privacy protections of the least secure site on which a user employs her account.[43] He argues that "while data portability may reduce vertical power imbalances between users and social network sites, it creates horizontal privacy trouble. Everyone who has access to 'portable' information on social network site A is now empowered to move that information to social network site B. In the process, they can strip the information of whatever legal, technical, or social constraints applied to it in social network site A."[44] Hence, personal data are only as secure as the least secure link in the chain through which they are transmitted.

On the other hand, data portability helps assuage an important risk of SNS walled gardens, the risk of lock-in and unfair competition. The network effect in the SNS market is so evidently strong, and reputational costs for users of switching services so steep, that as time passes a single SNS operator could gain sufficient market power to lock in users and stifle competition.[45] At the time this article is written, Facebook has 800 million users, 50 percent of whom log into the site on a daily basis. 250 million users access Facebook through their mobile devices.[46] To prevent the market from ossifying, competitive pressures must be sustained, if not by the power of markets then by regulation. For example, a consumer organization in the United States filed an antitrust complaint with the Federal Trade Commission arguing Facebook leveraged its power in the SNS market to shepherd subscribers to exclusively use its virtual currency.[47] Short of a full blown antitrust inquiry, mandating SNS operators to facilitate meaningful data portability could maintain competition despite the market's unavoidable network effects.

The antitrust argument could be countered, however, by SNS operators' claim to maintain some degree of control over their user base. SNS operators may argue that given that they do not harness a proprietary technology or protected patents, data portability could destroy their business model. Facebook, for example, invested significant effort in perfecting its user interface to make it attractive for users. Allowing users to simply walk away with their data and network intact may strip Facebook of an asset which is at least jointly created with the users themselves.

3. Aggregation vs. Disaggregation

An additional cost of credentials portability is its dampening effect on the ability of users to disaggregate their online identities by browsing anonymously or using pseudonyms. Credentials portability inevitably contributes to the development of a uniform aggregated online identity. I am identified as the same user across numerous websites and platforms; it is not "me, myself and I" but rather just "me". Moreover, SNS operators' real name policies mean that web interactions gradually become less anonymous.

To be sure, online anonymity has social costs. It is inversely correlated with accountability since it allows for harmful and deceptive self-identification, such as in the case of a child predator posing as a minor or a "troll" engaged in cyberbullying.[48] As Johnson, Crawford and Palfrey put it, "[w]e cannot trust

---

[43] James Grimmelmann, Saving Facebook, 94 Iowa L. Rev. 1137, 1194 (2009).
[44] Ibid.
[45] Randal Picker, Competition and Privacy in Web 2.0 and the Cloud (Univ. Chi. L. & Econ., Olin Working Paper No. 414, 2008), June 26, 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1151985.
[46] Facebook Statistics, September 1, 2011, http://www.facebook.com/press/info.php?statistics.
[47] Jia Lynn Yang, Facebook's virtual currency draws antitrust complaints from consumer advocates, Washington Post, June 29, 2011, http://www.washingtonpost.com/business/economy/facebooks-virtual-currency-draws-antitrust-complaints-from-consumer-advocates/2011/06/28/AG7cJypH_story.html.
[48] Strictly speaking, anonymity *can* be reconciled with accountability through products delivering "verified anonymity", such as Microsoft's U-Prove. U-Prove was developed by Stefan Brands and his company Credentica, since purchased by Microsoft, to act as an intermediary between users and websites, allowing users to share their personal information in a way that helps protect their privacy. U-Prove separates the retrieval of identity information from trusted organizations from the release of this information to destination sites. This prevents the issuing organizations from tracking where or when a user's information is used, and prevents destination sites from linking users' actions together. *See* Kaliya Hamlin, Bending the Identity Spectrum: Verifiable Anonymity at RSA, ReadWriteWeb, March 2, 2010, http://www.readwriteweb.com/archives/bending_the_identity_spectrum_verifiable_anonymity_rsa_security_conference.php.

each other unless we know whom we are trusting."[49] On the other hand, anonymity – and particularly anonymous communications – has been recognized as an important aspect of the right to privacy[50] and free speech.[51] Remaining anonymous is crucial for political speech in totalitarian regimes, where dissidents are often persecuted by a government actively seeking to unmask anonymous critics.[52] Yet it is also important in democratic societies, where individuals may be stymied from expressing views that are nonconforming, unconventional, or unpopular with their peers. For example, anonymity is necessary in order to shield whistleblowers inside corporations from retaliation by their superiors.[53] Dan Solove observes that "[a]nonymity and pseudonymity protect people from bias based on their identities and enable people to vote, speak, and associate more freely by protecting them from the danger of reprisal."[54] Accordingly, in NSTIC, the United States government promises that "the Identity Ecosystem will preserve online anonymity and pseudonymity, including anonymous browsing."[55]

While short of anonymity, disaggregation of identity remains a viable solution for users with pseudonymous identities.[56] Pseudonymity allows users to amass reputational capital while at the same time avoiding the aggregation of their identities under their real name.[57] With reputational capital comes increased accountability, since users have something to lose as a result of misbehavior.[58] SNS operators, however, explicitly ban use of pseudonyms and active disaggregation of user identities.[59] In its Statement of Rights and Responsibilities, Facebook not only requires users to use their real names but also forbids them from opening multiple accounts.[60]

---

[49] Johnson et al, *supra* note 21.

[50] Ruth Gavison disaggregated the right to privacy into three categories, "secrecy, anonymity and solitude." Ruth Gavison, Privacy, 89 Yale L.J. 421, 433 (1980). Alan Westin identified four "basic states of individual privacy": solitude; intimacy; anonymity; and reserve. Alan Westin, Privacy and Freedom 31-32 (1967).

[51] In McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995), the United States Supreme Court holds that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment." It notes that the Federalist Papers, authored jointly by James Madison, Alexander Hamilton, and John Jay between 1787 and 1788 were written under a pseudonym ("Publius"); ibid, at p. 343 n. 6. Accordingly, courts have imposed substantive and procedural burdens before allowing plaintiffs to unmask anonymous online counterparties. *See* Dendrite International v. Doe, 775 A.2d 756 (N.J. 2001); Doe v. Cahill, 884 A.2d 451 (Del. 2005); Solers, Inc. v. Doe, 977 A.2d 941 (D.C. 2009). Nathaniel Gleicher, John Doe Subpoenas: Toward a Consistent Legal Standard, 118 Yale L.J. 320 (2008). *Also see* recent decision of the Israeli Supreme Court: Civ. App. 4447/07 Mor v. Barak (March 22, 2010).

[52] *See, e.g.*, Mark Tran, Yahoo! sued over disclosure of Chinese citizens' identities, The Guardian, August 27, 2007, http://www.guardian.co.uk/world/2007/aug/28/china.news; *also see* Clive Thompson, Google's China Problem (and China's Google Problem), NY Times, April 23, 2006, http://www.nytimes.com/2006/04/23/magazine/23google.html.

[53] *See, e.g.*, Article 29 Data Protection Working Party, Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP 117, February 1, 2006, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf.

[54] Daniel Solove, A Taxonomy of Privacy, 154 U. Pa. L. REV. 477, 515 (2006).

[55] NSTIC, *supra* note 10, at p. 2.

[56] *See generally*, David Post, Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace, 1996 U. Chi. Legal F. 139.

[57] danah boyd argues pseudonymity is of particular value for weaker social groups, such as "abuse survivors, activists, LGBT people, women, and young people." She writes: "The people who most heavily rely on pseudonyms in online spaces are those who are most marginalized by systems of power. 'Real names' policies aren't empowering; they're an authoritarian assertion of power over vulnerable people." danah boyd, "Real Names" Policies Are an Abuse of Power, Apophenia, August 4, 2011, http://www.zephoria.org/thoughts/archives/2011/08/04/real-names.html; *also see* Jillian York, A Case for Pseudonyms, Electronic Frontier Foundation Blog, July 29, 2011, https://www.eff.org/deeplinks/2011/07/case-pseudonyms, arguing that "it is shortsighted for these companies to suggest that "real name" policies create greater potential for civility, when they only do so at the expense of diversity and free expression"; *but see* Berin Szoka, What's in a Pseudo-name? Privacy, Free Expression & Real Names on Google+ & Facebook, The Technology Liberation Front, August 29, 2011, http://techliberation.com/2011/08/29/whats-in-a-pseudo-name-privacy-free-expression-real-names-on-google-facebook/#more-38171.

[58] *See generally* Ken Kumayama, Note, A Right to Pseudonymity, 51 Ariz. L. Rev. 427 (2009).

[59] *See* discussion of Google's and Facebook's real name policies, *infra* notes 91 – 98 and accompanying text.

[60] *See* Facebook, Statement of Rights and Responsibilities, April 26, 2011, https://www.facebook.com/terms.php, providing: "Facebook users provide their real names and information (…) Here are some commitments you make to us relating to registering and maintaining the security of your account: (…) You will not create more than one personal profile".

The problem with such real name policies is that disaggregated identities linked to pseudonyms are no less "real" than aggregated identities associated with real names.[61] In the offline world, we are not forced to present the same "face," or identity, in all of our social interactions. We think, talk, and behave differently when we meet relatives, friends, dates, colleagues, business partners or our boss. Networking with colleagues on a business trip, we present quite a different persona than during a family dinner or on a trek to the Himalaya. In Online, however – and particularly in an ecosystem where identities become aggregated through credentials portability or otherwise – we are increasingly forced to present a uniform identity in all of our social interactions.[62] In addition, seldom are our offline expressions and actions as persistently attached to our identity as they are online – tagged, categorized and stored under our name. This is not natural and leads to what danah boyd called "privacy fails,"[63] or what Helen Nissenbaum views as fractures in contextual integrity.[64] It is what happens when identities that are typically presented in different contexts become conflated. Imagine "partygoer me" crashing into a business meeting that "I" am attending.[65]

Indeed, in most instances where SNS operators became involved in privacy snafus, they failed to respect disaggregated user identities. Consider the Google Buzz fiasco, where Google unilaterally implemented indiscriminate credentials portability to introduce Gmail users to a new social network. Users were horrified, and Google ended up paying dearly for mistakenly assuming that the "Gmail me" (i.e., the one who corresponds with a student, psychiatrist, or lover) could be merged by default with "myself" on Buzz (i.e., the one who communicates with friends or colleagues).[66] A few years earlier, Facebook mistook the "shopping me" for "SNS I", revealing through "Beacon" users' purchases on third party websites to their friends.[67]

Disaggregated identities do not even have to be pseudonymous. Technology can deliver disaggregation while users maintain a central identity in the background. Indeed, one of the most attractive features of Google's new SNS, Google Plus, is "Circles", which allows users to disaggregate their online identities with ease, sending updates to certain groups of people and not to others. A user can present a different identity to her high school friends, relatives, colleagues and followers, while at the same time continuing to use the same (assumingly real) name. Facebook, of course, provides similar functionality, although the user interface is not as intuitive as Google Plus'; is harder to navigate; and is set to present a uniform user identity by default to various categories of friends.[68] The conflation of circles

---

[61] Sherry Turkle writes that "the ability of the agent to represent herself as a different person in different online communities, without anyone being able to trace one identity to another, effectively creates multiple ways of knowing, which can be thought of as multiple selves." Sherry Turkle, Life on the screen: identity in the age of the Internet (Simon & Schuster; 1995). *Also see* Angel Adrian, No one knows you are a dog: Identity and reputation in virtual worlds, 24 Computer Law & Security Report 366 (2008).

[62] South Korea recently abandoned its nationwide real name plus resident registration number system for Internet users, following a security data breach involving theft of 35 million users' personal data. *See* Xinhua, South Korea plans to scrap online real-name system, China Daily, August 11, 2011, http://www.chinadaily.com.cn/world/2011-08/11/content_13095102.htm.

[63] danah boyd, Making Sense of Privacy and Publicity, SXSW, March 13, 2010, http://www.danah.org/papers/talks/2010/SXSW2010.html.

[64] Helen Nissenbaum, Privacy as Contextual Integrity, 79 Wash. L. Rev. 119 (2004); Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010).

[65] One commentator states: "Persistent pseudonyms aren't ways to hide who you are. They provide a way to be who you are." Kee Hinckley, On Pseudonymity, Privacy and Responsibility on Google Plus, TechnoSocial Blog, July 27, 2011, http://www.marrowbones.com/commons/technosocial/2011/07/on_pseudonymity_privacy_and_re.html.

[66] Amir Efrati, Google Settles Privacy Lawsuit for $8.5 Million, Wall Street Journal, Sept. 3, 2010, http://online.wsj.com/article/SB10001424052748703946504575470510382073060.html; Julia Angwin& Amir Efrati, Google Settles With FTC Over Google Buzz, Wall Street Journal, Mar. 31, 2011, http://online.wsj.com/article/SB10001424052748703806304576232600483636490.html.

[67] Jon Brodkin, Facebook Halts Beacon, Gives $9.5M to Settle Lawsuit, PC World, December 8, 2009, http://www.pcworld.com/article/184029/facebook_halts_beacon_gives_95m_to_settle_lawsuit.html.

[68] *See* Jacqui Cheng, One month with Google+: why this social network has legs, Ars Technica, August 7, 2011, http://arstechnica.com/web/news/2011/08/one-month-with-google-why-the-social-network-has-legs-1.ars, stating: "I was one of the first people to loudly declare that you can do the same thing on Facebook, but so few people know this that it's basically a nonexistent feature; that's the problem with Facebook. With Google Plus, sending out certain updates to some people and other updates to other people is right at the forefront of the experience. You are always asked to make a conscious decision about your social circles and about which circles get to see which posts". For Facebook's latest attempt to increase user control over identity, *see* Somini Sengupta, New Control over Privacy on Facebook, NY Times, August 23, 2011, http://www.nytimes.com/2011/08/24/technology/facebook-aims-to-simplify-its-privacy-settings.html?_r=1.

of acquaintances on Facebook is a liability, since counter to Facebook's ethos of increased sharing it causes users to hold back personal content, in fear of overexposure to colleagues; as well as professional content, in fear of boring their relatives and friends.69 It also impacts Facebook's neutrality as a steward of identity,[70] since by displaying professional updates to friends and relatives, Facebook could cause a user to rapidly decline in popularity and see her posts demoted on her friends' News Feeds.[71]

A potential retort to the promotion of disaggregated identities as a mechanism for user control over the dissemination of information is that content posted to a certain group can in any event seep through to other groups. Yet this problem does not negate the utility of disaggregation. We should not confuse the concept of secrecy with that of privacy and user control. As Dan Solove explains, under a secrecy paradigm, a privacy violation occurs only when concealed data is revealed to others; whereas if information is voluntarily turned over to a third party, there is no longer a reasonable expectation of privacy.[72] This paradigm is overly narrow and based on a series of United States Supreme Court cases which viewed voluntary disclosure of information as an "assumption of risk" negating the right to privacy.[73] In Europe, the whole thrust of data protection law pertains to the fair and lawful use of information by third parties; hence legal protection begins in Europe where it ends in the United States.[74] While information disclosed by users to a certain group of contacts could conceivably find its way to additional third parties (SNS contacts or not), the same could happen offline. For example, a relative participating in a party you attended can tell your boss she saw you get drunk. Offline as online, worlds can collide. Yet with disaggregated identities, users can maintain a certain degree of control over their information, as they do offline. That is a worthy goal to pursue.

4. Neutrality

SNS operators benefit from a wide degree of control over numerous attributes of user identities. They can influence how one is portrayed online – as a warm family man or an ambitious professional; an art-loving bohemian or a wine connoisseur. To be sure, some decisions with respect to the content posted or uploaded by users are subject to user control. For example, a user can decide whether or not she will upload a photo to a SNS or identify another user as a friend or relative. However, many other decisions remain in the sole domain of SNS operators with very little transparency for users. This includes the handling of "meta data" concerning users' interaction with the SNS; whose profiles a user viewed; whom she was tagged with; how long she lingered on a page; which links she "liked" or clicked through; what content she was interested in; which devices she used; and what locations she visited.[75] It also includes deciding which information will be promoted and featured prominently for others to see and which pushed down and therefore relegated to oblivion.[76] Facebook, for example, uses algorithms to filter users' News Feeds to only show content from people Facebook determines they are most interested in. The implications are clear: Users will view me as a family man if they see the pictures I upload of my kids; as a professional if they see my legal updates. Facebook's control over the digital curation of users' identity has recently deepened with the merging of the "Top News" and "Most Recent" tabs in the News Feed into a single column.[77]

---

[69] "I'm not under the illusion that all my selves are equally appealing, though, and this was where I got confused to the point of paralysis. Would my profile reflect Professional Writer Curtis (upbeat, friendly, responsible) or Real Curtis (disagreeable, slovenly, judgmental)? Would I use it to hawk my books, or to post pictures of my baby eating her toes? I know the obvious answer is both, but — call me old-fashioned — that just feels completely weird." Sittenfeld, *supra* note 2.

[70] *See infra* Part 4.

[71] Sittenfeld, *supra* note 2.

[72] Daniel Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477, 497 (2006).

[73] United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979); *see* discussion in Omer Tene, What Google Knows: Privacy and Internet Search Engines, 2008 Utah L. Rev. 1433, 1470-74.

[74] *See* Omer Tene, Privacy in Europe and the United States: I Know It When I See It, CDT Blog, June 27, 2011, http://www.cdt.org/blogs/privacy-europe-and-united-states-i-know-it-when-i-see-it.

[75] *See* Kashmir Hill, Anonymous Facebook employee dishes the privacy dirt, Forbes, January 11, 2010, http://www.forbes.com/sites/kashmirhill/2010/01/11/anonymous-facebook-employee-dishes-the-privacy-dirt.

[76] Kashmir Hill, Resisting the algorithms, Forbes, May 5, 2011, http://www.forbes.com/sites/kashmirhill/2011/05/05/resisting-the-algorithms.

[77] Facebook Help Center, Updates to News Feed, http://www.facebook.com/help/?page=189712557768134. *See*

Why do Joe's wall posts appear at the top of his friends' News Feed, while Jane's remain discrete and visible by only her mother? Who will get Jerry's Google Plus postings on their Stream and who will not? The answers to these questions are left to conjecture based on opaque statements of SNS operators.[78] For example, in its Help Center Facebook replies to the question "How does News Feed determine which content is most interesting?" as follows: "The News Feed algorithm bases this on a few factors: how many friends are commenting on a certain piece of content, who posted the content, and what type of content it is (*e.g.*, photo, video, or status update)."[79] This explanation provides precious little information about the logic and considerations underlying Facebook's decision-making process. Is Facebook motivated by commercial interests? Political considerations? Could its decisions be arbitrary? Mistaken? Is Facebook "neutral"? We simply do not know.

Our SNS identity consists of the sum of our activity on and interaction with the service. The fact that SNS operators enjoy a great degree of control over complete vectors of our identity is troubling. Transparency,[80] accountability,[81] and user control[82] are fundamental principles of privacy and data protection law in Europe and elsewhere. Each of these principles is challenged by the delegation of control over online identity to unaccountable actors.

To be sure, algorithms determining which content to promote or search results to display are proprietary trade secrets of SNS operators. Forcing SNS operators to disclose these algorithms would dampen innovation. Yet there is a clear feeling that we deserve more than we are getting.[83] Consider Article 12 of the European Data Protection Directive, which provides that "Member States shall guarantee every data subject the right to obtain from the controller (…) knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions (…)". How

---

discussion in Jason Kincaid, Facebook News Feed Gets Smarter— And the Ticker Makes its Big Debut, Techcrunch, September 20th, 2011, http://techcrunch.com/2011/09/20/facebook-news-feed-gets-smarter%E2%80%94%C2%A0and-the-ticker-makes-its-big-debut.

[78] *See, e.g.*, Thomas E. Weber, How Facebook Decides What To Put In Your News Feed – These 10 Secrets Reveal All, Business Insider, 18 October 2010, http://www.businessinsider.com/how-facebook-decides-what-to-put-in-your-news-feed--these-10-secrets-reveal-all-2010-10.

[79] Facebook Help Center, "How does News Feed determine which content is most interesting?", http://www.facebook.com/help/?faq=166738576721085.

[80] The transparency (or openness) principle appears in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Sep. 23, 1980, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (the "OECD Guidelines"); as well as in the Articles 10-11 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 (European Data Protection Directive); and numerous privacy and data protection laws around the world.

[81] The accountability principle appears in the OECD Guidelines as well as in Canada's federal privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), (S.C. 2000, c. 5), Schedule 1, Principle 4.1, titled "Accountability"; though not in the European Data Protection Directive. This may soon change, as the European Data Protection Directive is being reviewed and the introduction of an accountability principle pursued by both the European Commission and the Article 29 Data Protection Working Party. *See* European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive strategy on data protection in the European Union, Brussels, COM(2010) 609, November 4, 2010, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf ("Commission Communication"); Article 29 Data Protection Working Party, Opinion /2010 on the principle of accountability, WP 173, July 13, 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf; Article 29 Working Party, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, December 1, 2009, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf. *Cf.* in the United States, Department of Commerce Internet Policy Task Force, Green Paper on Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, December 16, 2010, http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf (the "Green Paper").

[82] The user control (or consent) principle is a fundamental building block of any privacy and data protection legislation. *See* Articles 7(a) and 8(2)(a) of the European Data Protection Directive; Schedule 1 Principle 3 of the PIPEDA; the Green Paper. For the "notice and choice" framework in the United States, *see* Preliminary FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[83] Beth Simone Noveck, Trademark Law and the Social Construction of Trust: Creating the Legal Framework for Online Identity, 83 Wash. U. L. Q. 1733, 1778-79 (2005), arguing that "[i]f I am to be accorded a reputational score, I ought to know what the criteria are".

exactly does an SNS operator determine who our best friends are and which content to display on our News Feed?

The (lack of) neutrality problem was explored by Eli Pariser in his book "The Filter Bubble: What the Internet Is Hiding from You".[84] Pariser thinks that increased personalization of the Internet, in search, advertising and SNS, poses a risk to open society and democratic discourse. He explains that if you have hundreds of Facebook friends, you will see relevant updates from only a subset of them that Facebook deems "closest". This effectively compartmentalizes society into pockets (or echo chambers) of likeminded individuals sharing similar backgrounds. For example, conservatives will only see content posted by fellow conservatives, while updates from their liberal acquaintances – even if they "friend" them – will be suppressed.[85] Pariser believes government should regulate information intermediaries to ensure users have full control over their data.

More troubling, as the Internet's "social layer" evolves, editorial control of SNS operators extends beyond the walled garden of the SNS to the open Internet. Bing recently announced: "Starting today, you can receive personalized search results based on the opinions of your friends by simply signing into Facebook (…). Decisions can now be made with more than facts, now the opinions of your trusted friends and the collective wisdom of the Web."[86] Hence, Facebook promotion or demotion of content posted to the site by users will now affect not only the profiles of those users but also the search results yielded by their friends. In addition, SNS identities are increasingly harnessed for important offline decisions in the field of employment, insurance or credit.[87] The New York Times recently reported that "Companies have long used criminal background checks, credit reports and even searches on Google and LinkedIn to probe the previous lives of prospective employees. Now, some companies are requiring job candidates to also pass a social media background check."[88] The treasure trove of information about job candidates, employees, loan or insurance applicants, and prospective tenants, is too attractive for businesses to ignore.[89] This means that the stakes are becoming higher for users, even as control over their SNS identity withers.[90]

5. Deletion

When users create content on platforms owned by SNS operators, they grant operators a great deal of control over what they have produced. Users who make Facebook or Google Plus their primary online presence deposit something of great economic and emotional value with those SNS operators. They

---

[84] Eli Pariser, The Filter Bubble: What the Internet Is Hiding from You (Penguin, 2011).

[85] This phenomenon, sometimes referred to as "cyberbalkanization" (*see* Wikipedia entry, http://en.wikipedia.org/wiki/Cyberbalkanization), was originally explored by Cass Sunstein, Republic.com (Princeton University Press, 2001); *also see* Andrew Shapiro, The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know (PublicAffairs, 2000).

[86] The Bing Team, Facebook Friends Now Fueling Faster Decisions on Bing, Bing Search Blog, 16 May 2011, http://www.bing.com/community/site_blogs/b/search/archive/2011/05/16/news-announcement-may-17.aspx.

[87] Jeffrey Rosen, The Web Means the End of Forgetting, NY Times, 21 July 2010, http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.

[88] Jennifer Preston, Social Media History Becomes a New Job Hurdle, NY Times, July 20, 2011, http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html?pagewanted=all; Jenna Wortham, More Employers Use Social Networks to Check Out Applicants, NY Times, August 20, 2009, http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants.

[89] *See, e.g.*, James Brown, Insurers use social networking sites to identify risky clients, The Other James Brown, November 30, 2010, http://blogs.msdn.com/b/james_brown/archive/2010/11/30/insurers-use-social-networking-sites-to-identify-risky-clients.aspx.

[90] One way to address these issues is by laws limiting the permitted uses of information harvested from SNS, such as employment discrimination laws or credit reporting regulation. For example, California has recently adopted a new statute which clarifies that jurors may not use SNS to research or disseminate information about cases, and can be held in criminal or civil contempt for violating these restrictions. *See* 2011 Cal. Laws chap. 181. *Also see* Omer Tene, What happens online stays online: Comments on "Do Not Track", Stanford CIS Blog, March 26, 2011, http://cyberlaw.stanford.edu/node/6645. Beth Noveck suggests drawing from legal protections for credit scores to legal protections for online identity. Noveck, *supra* note 83, at p. 1767, 1782.

delegate to Facebook or Google stewardship over their digital identity. This has two important implications.

First, the prospect of having such identity intentionally or accidentally deleted is disconcerting. In its efforts to enforce its "real name policy," which forbids pseudonymous profiles, Google recently deleted a large number of user profiles allegedly not using "real" names.[91] Mashable reported that "while some of the suspended accounts were indeed fake profiles, others like Limor 'Ladyada' Fried and lifestyle blogger A.V. Flox were accidentally deleted and quickly restored."[92] A wave of angry user blog posts prompted Google to amend its procedure for enforcement of its real name policy, providing users with a four-day "grace period" to fix a profile name before any further action is taken.[93] If a profile is suspended for a names violation, Google has been reported to require users to verify their identity by presenting either government issued identity documentation or a link to a profile on another social network with a similarly strict naming policy, like Facebook.[94] Facebook too enforces a real name policy and has been known to delete pseudonymous accounts.[95] In one recent case, Facebook deleted the profile of Zhao Jing, better known as Michael Anti, a Chinese human rights activist, despite his extensive activity as a dissident under that name over the course of many years.[96] The loss of the network of contacts, as well as the links, updates and photos posted to a SNS can be devastating.[97] Internet scholar danah boyd explains that "even when folks have a negative reputation, they often don't want to lose the positive reputation that they've built. Starting at zero can be a lot harder than starting with a mixed record."[98]

The second implication is that users should benefit from the autonomy to terminate their accounts and delete their profiles at will. One of the earliest public controversies surrounding Facebook concerned its account deletion policy. While users could deactivate their accounts, they were not able to delete content accumulated in their profile from Facebook servers.[99] In February 2008, as a result of public criticism and an inquiry by the United Kingdom's Information Commissioner's Office, Facebook began to allow users to permanently delete their accounts. Currently, Facebook explains in its privacy policy: "If you want to stop using your account you may deactivate it or delete it. When you deactivate an account, no user will be able to see it, but it will not be deleted. (…) We save your profile information (connections, photos, etc.) in case you later decide to reactivate your account. (…) When you delete an account, it is permanently deleted from Facebook."[100]

The ability to shed an online identity or disengage from a SNS sparked public controversy following the suggestion of Google's (then) CEO Eric Schmidt that "every young person one day will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored

---

[91] Violet Blue, Google Plus Deleting Accounts En Masse: No Clear Answers, ZD Net, July 23, 2011, http://www.zdnet.com/blog/violetblue/google-plus-deleting-accounts-en-masse-no-clear-answers/567.

[92] Ben Parr, Google Responds to Google Plus Account Suspension Controversy, Mashable, July 26, 2011, http://mashable.com/2011/07/26/google-plus-common-names.

[93] Saurabh Sharma, Google Plus Blog, August 11, 2011, https://plus.google.com/109179785755319022525/posts/YcvRKqJeiZi.

[94] Tim Carmody, Google Plus Punts on Kafkaesque Name Policy, Wired Epicenter, August 12, 2011, http://www.wired.com/epicenter/2011/08/google-punts-names/all/1.

[95] *Supra* note 60.

[96] Tini Tran, Activist Michael Anti Furious He Lost Facebook Account--While Zuckerberg's Dog Has Own Page, Huffington Post, March 8, 2011, http://www.huffingtonpost.com/2011/03/08/michael-anti-facebook_n_832771.html.

[97] Notice that while I emphasize account deletion as a result of names violations, SNS operators have deleted user accounts for spam or abuse or other "community violations".

[98] danah boyd, a few thoughts on name changes & reputation, apophenia, August 16, 2010, http://www.zephoria.org/thoughts/archives/2010/08/16/name-changes-reputation.html.

[99] Maria Aspan, How Sticky Is Membership on Facebook? Just Try Breaking Free, NY Times, February 11, 2008, http://www.nytimes.com/2008/02/11/technology/11facebook.html?_r=1&ref=business&oref=slogin; *also see* Steve Mansour, 2504 Steps to closing your Facebook account, Steve Mansour Blog, July 23, 2007, http://www.stevenmansour.com/writings/2007/jul/23/2342/2504_steps_to_closing_your_facebook_account.

[100] Facebook Site Governance, Privacy Policy: How You Can Change or Remove Information, March 26, 2010, http://www.facebook.com/note.php?note_id=10150162293220301; *also see* Elizabeth Denham, Assistant Privacy Commissioner of Canada, PIPEDA Case Summary #2009-008, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act, July 16, 2009, http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.

on their friends' social media sites."[101] danah boyd was not amused: "This is ludicrous on many accounts. First, it completely contradicts historical legal trajectories where name changes have become increasingly more difficult. Second, it fails to account for the tensions between positive and negative reputation. Third, it would be so exceedingly ineffective as to be just outright absurd."[102] Schmidt's comment was generally depicted[103] as (another)[104] snide remark from the head of a company which utilizes personal data as raw material for its products and services.[105] In fact, however, Schmidt's prediction echoes a proposal by another Internet thought leader, Jonathan Zittrain, to allow individuals to declare "reputational bankruptcy".[106] Zittrain suggests that as identity grows in importance on the Internet, "the intermediaries demanding it ought to consider making available a form of reputation bankruptcy. Like personal financial bankruptcy, or the way in which a state often seals a juvenile criminal record and gives a child a 'fresh start' as an adult, we ought to consider how to implement the idea of a second or third chance into our digital spaces."[107] Hence, not unlike Schmidt, Zittrain proposes providing users with a chance for a reputational fresh start.

The concept of reputational bankruptcy, in turn, is related to a debate raging over the past year or so on both sides of the Atlantic with respect to the so called "right to be forgotten," better known in French as the *droit d'oubli*.[108] In its Communication on "A comprehensive approach on personal data protection in the European Union", the European Commission expressed its intention to "clarify[…] the so-called 'right to be forgotten', i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes."[109] Similarly, EU Justice Commissioner Vivienne Reding stated: "Peoples' rights need to be built on four pillars: The first is the 'right to be forgotten': a comprehensive set of existing and new rules to better cope with privacy risks online."[110] Thus, the right to be forgotten has emerged as a central tenet of the reshaping European data protection framework.

To some extent, a right to be forgotten already exists under Article 6(1)(e) of the Data Protection Directive, which provides that "Member States shall provide that personal data must be: (…) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."[111] Yet it would be risky to extend the existing provision to accommodate a full blown right to be forgotten. First, even the currently existing provision requires a delicate balancing act between the obligation to delete data and a multitude of data retention requirements; such as those in anti-money laundering acts, communications data retention legislation, or United States electronic discovery regulations.[112] Businesses often find themselves in a

---

[101] Holman W. Jenkins, Google and the Search for the Future, August 14, 2010, http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html.
[102] boyd, *supra* note 98.
[103] Kyle Thibaut, Eric Schmidt's Name Game Doesn't Make Sense, Techcrunch, August 16, 2010, http://techcrunch.com/2010/08/16/eric-schmidt-change-name/.
[104] Google CEO on Privacy (VIDEO): 'If You Have Something You Don't Want Anyone To Know, Maybe You Shouldn't Be Doing It', Huffington Post, December 7, 2009, http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html.
[105] Tene, *supra* note 73.
[106] Zittrain, *supra* note 4, at p. 228-29; *also see* Lior Jacob Strahilevitz, "How's My Driving?" For Everyone (and Everything?), 81 N.Y.U. L. Rev. 1699, 1736 (2006), stating: "Online reputation sites suffer somewhat because users with poor reputations can always 'flush' their existing identities and start over with a blank slate".
[107] Jonathan Zittrain, Reputation bankruptcy, Concurring Opinions, September 7, 2010, http://www.concurringopinions.com/archives/2010/09/reputation-bankruptcy.html.
[108] Natasha Singer, Just Give Me the Right to Be Forgotten, NY Times, August 20, 2011, http://www.nytimes.com/2011/08/21/business/in-personal-data-a-fight-for-the-right-to-be-forgotten.html.
[109] Commission Communication, *supra* note 81.
[110] Viviane Reding, Your data, your rights: Safeguarding your privacy in a connected world, Privacy Platform "The Review of the EU Data Protection Framework", Brussels, March 16, 2011,
[111] Jeremy Warner, The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps, 2 U. Ottawa L. & Tech. J. 75 (2005).
[112] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54. *See generally* Francesca Bignami, Privacy and Law Enforcement in the European Union: The Data Retention Directive, 8 Chi. J. Int'l L. 233 (2007); Article 29 Data Protection Working Party, Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the

quagmire trying to assess whether they are obliged to delete or retain data; for how long; and for which purposes.[113] Second, the right to be forgotten is often a euphemism for a "right to delete negative information published about you". Few people are interested in getting rid of positive information. Hence, the right to be forgotten may be better phrased as a "right to have your sins forgotten", protecting not so much privacy but rather reputation. As Jeffrey Rosen puts it: "What people seem to want is not simply control over their privacy settings; they want control over their online reputations. But the idea that any of us can control our reputations is, of course, an unrealistic fantasy."[114] Third, despite the ongoing public debate, there is persistent lack of clarity with respect to the specifics (let alone mechanics) of the right to be forgotten. Sure enough, you should be able to delete a photo you posted on your SNS profile; but should you be authorized to delete a photo of you that I post on *my* SNS profile? Or request that Google suppress a link to a photo you initially posted but that is currently echoed on various third party websites? Or if you post a comment on your profile and I copy it onto my profile, could you demand that I delete it?[115] Clearly, implementing such a right would implicate potential conflicts with freedom of speech as well as the rules on intermediary liability. Finally, consider that while the right to be forgotten benefits individuals with minor vices, it also facilitates more malicious behavior, such as "trolling" and then deserting an account.[116] Lior Strahilevitz warns that "users with poor reputations can always 'flush' their existing identities and start over with a blank slate."[117] Consequently, there is inherent tension between the right to be forgotten and the accountability of online actors. [118]

6. Conclusion

The Internet is a giant shopping mall, library, town square, dating site, government arena, outlet for free speech and political dissent, and much more. Digital identity is used online not only in contexts requiring strong authentication, but also in less formal interactions where anonymous, pseudonymous, and disaggregated identities can suffice. Increasingly, SNS operators are harnessing their broad user base and wealth of personal information to become vital components of the Internet's identity layer. The provision of identity management tools by SNS operators for purposes of authentication, identification and authorization raises thorny problems of privacy, security and user control.

SNS operators can influence how users are portrayed online, raising question marks with respect to their neutrality. Credentials portability, while enhancing transactional efficiencies, creates privacy concerns, as user data from third party websites is amalgamated by SNS operators. Data portability reduces risk of lock in and concentration of power but challenges the protection of third parties' personal data under shifting privacy policies. The power to delete a user's profile is key, ranging from SNS operators' deletion of pseudonymous user accounts to users' claiming a "right to be forgotten" with respect to content stored on a SNS. The optimal mix of features would allow SNS operators to provide credentials portability while at the same time letting users maintain disaggregated identities and obtain authorizations on an anonymous or pseudonymous basis.

---

provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, March 25, 2006, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf.

[113] *See, e.g.*, Bridget Treacy, US e-discovery obligations v. EU data protection laws: a conundrum for businesses, Complinet, February 12, 2008, http://www.hunton.com/files/Publication/0ba5b3ee-be3d-4438-a3e7-54962af9b74b/Presentation/PublicationAttachment/84ba39e7-3ba6-43b9-96cc-1dd5b1e05dfb/Treacy_US_e-discovery_2.08.pdf.

[114] Rosen, *supra* note 87.

[115] *See* discussion by Google Privacy Lead Peter Fleischer, Foggy thinking about the Right to Oblivion, Peter Fleischer: Privacy…? Blog, March 9, 2011, http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html; Peter Fleischer, "The Right to be Forgotten", seen from Spain, Peter Fleischer: Privacy…? Blog, September 5, 2011, http://peterfleischer.blogspot.com/2011/09/right-to-be-forgotten-seen-from-spain.html.

[116] Mattathias Schwartz, The Trolls among Us, NY Times, August 3, 2008, http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html.

[117] Strahilevitz, *supra* note 106.

[118] Johnson et al, *supra* note 21, at p. 82.

.* * * * *

Cite as: Tene, Omer. "Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services.*Journal of International Commercial Law and Technology,* Vol.8 No.2 (April,, 2013)