Regulating the Man Behind the Curtain

by

Christina M. Gagnier, Esq.

"Pay no attention to the man behind the curtain!"

- Frank L. Baum, *The Wonderful Wizard of Oz*

Frank L. Baum's famed novel, *The Wonderful Wizard of Oz,* has been noted as a political allegory for the gold standard amongst other speculation as to Baum's intentions when penning the beloved children's tale. While the early twentieth century novel was written at a time when the conception of privacy itself was nascent, with Samuel Warren and Louis Brandeis' often-cited *The Right to Privacy* being written for Harvard Law Review a mere ten years before, the title character, the Wizard of Oz, the "man behind the curtain," serves as an appropriate analogy for exploring the practice employed by many of the world's most famous brands today of managing Internet user data through the use of third-party "social network intermediary" systems.[1]

The Wizard of Oz is an unknown entity for much of the 1900 novel: he appears in multiple incarnations, but his true nature does not become clear until near the end of the story. He is simply a "man behind the curtain," using machines, illusions and gadgetry unknown to the public on the other side. Despite the illusion, many of the world's most popular brands are not directly interacting with Internet users through their own means on social networks like Twitter, Facebook and YouTube. Their communication is powered by the use of social network intermediaries, third party systems that allow for brands to manage all communications about or with them on multiple social network services across the social Web. While these brands may be using these third party services, the Internet user has no clue as to their existence: these services are a hidden party unknown to the Internet user.

While these social network intermediaries operate legally under arguably some of the strictest standards, such as the 1995 European Privacy Directive, those who constructed this regulation could not have envisioned their existence.[2] Today, as the "right to be forgotten" online is being debated in the European Union, the existence of these social network intermediaries, these "man behind the curtain" systems, may threaten the ability of Internet users to fully preserve their rights.

Why should we care that third parties are processing data that has already been made publicly available by Internet users? It cannot be overlooked that these social network intermediaries do not merely "process" and "store" data. Their systems take publicly available data, and by aggregating Internet users activity across multiple social networks, they enable brands to create a profile of these Internet users and all of their interactions. While the original data may be publicly available,

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard L. Rev. 193 (1890).
[2] Council Directive 95/46, 1995 O.J. (L 281) 0031-0050 (EC).

these systems allow for aggregation, commentary, campaigns and brand interactions that form an entirely new set of data that the brand gets to leverage and the intermediary has to store.

The unsettling legal existence of the social network intermediary should be examined in three ways: 1) the ability of the social network intermediary to give meaningful notice to the Internet user whose data is being processed; 2) the ability of the social network intermediary to gain meaningful consent from the Internet user; and 3) the ability of the social network intermediary to engage in data deletion for those Internet users who wish to "be forgotten."

Giving Meaningful Notice and Gaining Meaningful Consent

Much like the man behind the curtain, the social network intermediary's intent is to remain unknown: their business purpose is to empower brands to look like they are masters of social media and public relations in this digital age. This invisibility to the Internet user, however, smacks against society's notions, regulatory and normative, of meaningful notice and consent when it comes to the collection, management and storage of data.

The classic method of notice, the privacy policy, is rendered wholly ineffective since the Internet user does not know where to go to even find it. Alternate notice mechanisms, as discussed in the literature regarding notice, may also be ineffective for the same reason since the Internet user is likely unaware the third party even exists.[3] The consent problem is relatively straightforward: I cannot say "yes" or " no" if I do not know that you exist.

These social network intermediaries have the same obligations as any other company to comport with domestic and international privacy laws. Many of the companies that operate as social network intermediaries, in fact, do have privacy policies and comply with international privacy standards. In searching the Department of Commerce's EU-US Safe Harbor database of companies that are certified as complying with the 1995 EU Privacy Directive, you can find many of these U.S.-based companies listed as being Safe Harbor compliant.[4] While these companies may have done what they needed to do to comply with the letter of existing laws, the spirit of these laws is not honored since the Internet user does not know the social network intermediary is operating with their information, even if it is publicly available.

The EU Data Privacy Directive appears to account for this relationship between the brand and the social network intermediary: it has set out requirements and obligations for data controllers, those who may be the original source of data input, and companies who act as data processors, merely providing the vehicle for the data to be manipulated within.[5] There is a meaningful distinction when it comes to social network intermediaries between the entity that controls the data in question and the entity that merely processes it. Practically, when the social network intermediary's relationship is executed with the brand, through a vendor contract, normally a licensing agreement of some sort for platform use, it is usually accompanied by a Data

[3] M. Ryan Calo, *Code, Nudge or Notice?,* University of Washington School of Law Research Paper No. 2013-04 (February 13, 2013).
[4] Department of Commerce, EU-US Safe Harbor Home Page, available at http://export.gov/safeharbor/eu/eg_main_018365.asp.
[5] Council Directive 95/46, 1995 O.J. (L 281) 0031-0050 (EC).

Transfer Agreement (DTA) that is executed with provisions known as the Standard Contractual Clauses.[6] These clauses painfully detail the obligation of the data controller and the data processor as well as what types of information are applicable to cross-border transfer in that particular situation.

While the obligations may be clear to the parties involved in the contractual relationship, the public's inability to know of the existence of all parties strips them of their rights to voice concerns or file grievances with the appropriate authorities under these agreements, such as the Federal Trade Commission (FTC), the European data protection authorities (DPAs) or the Swiss Federal Data Protection and Information Commissioner (FDPIC). The reasonable expectation of the data subjects, the Internet user, has received limited treatment as to the liability assigned between the controller and the processor vis-à-vis one another, but this reasonable expectation must also be considered generally in terms of the public's ability to understand the relationship of all companies involved with their data, public or private.[7]

To Be Forgotten: Advances in the European Union's Approach to Data Privacy

The ultimate form of "opting out" of a platform or online system is currently being debated in Europe: data deletion. The European Commission has been exploring comprehensive reform of the EU data protection rules, incorporating the inclusion of the "right to be forgotten."

If such regulation came to pass, data controllers and processors would likely be required to delete the information of users who no longer desired to have their information stored. Spain is already enforcing the "right to be forgotten" when it comes to data that is publicly available through search engines.[8] Spain's Data Protection Agency has ordered search engine Google to delete links and information on nearly ninety people, action that Google continues to challenge. Artemi Rallo, the Director of the Spanish Data Protection Agency makes a fair point: "Google is just 15 years old, the Internet is barely a generation old and they are beginning to detect problems that affect privacy. More and more people are going to see things on the Internet that they don't want to be there."[9]

All of the cases involving Google share the same genesis – the individuals petitioned the Spanish agency to have the information removed from Google's index. While it is apparent in the case of Google that it was Google that had the power to remove the information about the individuals (after all, they did "google" to find the information about themselves), the data deletion involved in the "right to be forgotten" is contingent upon a party having knowledge of all parties involved in controlling the destiny of their data.

In the case of the social network intermediary, enforcement of data deletion would be reliant on the data controller communicating to the data processor that a particular individual's data

[6] Commission Decision, 2010/87/EU, 2010 O.J. (L 39) 5-6, 11 (EU).
[7] Article 29 Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (WP 128, 22 November 2006).
[8] AOL News, Fox News Latino, *Spain Asserts a 'Right to be Forgotten,' Ordering Google to Remove Some Old Links*, April 21, 2011, available at http://noticias.aollatino.com/2011/04/21/right-to-be-forgotten-google/.

[9] *Id.*

must be deleted. The Internet user would be counting on the brand to communicate to the social network intermediary to delete the information. While this obligation is something that could arguably be embedded into the amended regulatory framework, its' practical application is something else altogether. It assumes that the brand companies have invested in robust privacy practices and training practices for their employees who are on the front lines managing these requests. It also assumes that the social network intermediary has done the same.

The right to be forgotten currently faces a variety of challenges, but its adoption, which may take place in 2014, would pose issue for the uncomfortable existence of the intermediary and their responsibility to the Internet user.[10]

What To Do With That Which is Already Public

"Oh, no my dear. I'm a very good man. I'm just a very bad Wizard."

- Frank L. Baum, *The Wonderful Wizard of Oz*

The world's greatest brands utilize social network intermediaries to remain the world's greatest brands. They seek to have relationships and a level of responsiveness to the would-be consumer or fan that would not be possible without the existence of the social network intermediary's powerful "social" platform. Is it that big of a deal that brands want avenues to connect to their most loyal fans on the Web?

Society's privacy debate, as its core, is about trust in relationships. Internet users want to be able to know that the data they put out about themselves online is only being used by parties that they have given consent to and is not being used in a manner or by a party they are unaware of.

Brands using social network intermediaries are hiding something: they are concealing the fact that a third party is involved in the relationship, the man behind curtain. Their privacy policies, if they even exist, may give notice that they are using "third party services" to effectuate their relationship with their consumers and the general public, but most often they do not disclaim who these third parties are.

It must not be forgotten that the data being discussed as subject to protection has already been made public. It is data that is already out in the wild and voluntarily so. Is it not just waiting to be reigned in?

The privacy we hope to enjoy is in the perception. We believe these interactions are happening directly with the brands we Like and Tweet, not the "man behind the curtain." We believe that our favorite brands have a Twitter account, and, perhaps these interactions are being stored by Twitter, but that is where it ends. Twitter has a data deletion policy; these social network intermediaries may not. In the civil law world where privacy is based on norms, perception is everything. If we look behind the curtain, we might not like what we see.

[10] Eric Pfanner, *Archivists in France Fight a Privacy Initiative*, The New York Times, June 16, 2013, available at http://www.nytimes.com/2013/06/17/technology/archivists-in-france-push-against-privacy-movement.html?pagewanted=all.