2014

"All Data is Credit Data," or, On Close Reading as a Reciprocal Process in Digital Knowledge Environments

John Hunter
jchunter@bucknell.edu

"All Data is Credit Data," or, On Close Reading as a Reciprocal Process in Digital Knowledge Environments

Scholarly and Research Communication
VOLUME 5 / ISSUE 2 / 2014

John C. Hunter
Bucknell University

Abstract
The new knowledge environments of the digital age are often described as places where we are all closely read, with our buying habits, location, and identities available to advertisers, online merchants, the government, and others through our use of the Internet**.** This is represented as a loss of privacy in which these entities learn about our activities and desires, using means that were unavailable in the pre-digital era. This article argues that the reciprocal nature of digital networks means 1) that the privacy issues that we face online are not radically different from those of the pre-Internet era, and 2) that we need to reconceive of close reading as an activity of which both humans and computer algorithms are capable.

Résumé
Les nouveaux environnements de connaissance de l'ère numérique sont souvent décrits comme les endroits où nous sommes tous de près lus, avec nos habitudes d'achat, endroit et identités disponibles pour les publicitaires, les négociants en ligne, le gouvernement et d'autres par notre utilisation d'Internet; c'est une perte de vie privée dans laquelle ces entités apprennent de nos activités et désire utiliser des moyens qui étaient non disponibles dans l'ère pré-numérique. Cet article soutient que la nature réciproque de moyens de réseaux numériques 1) que les éditions de vie privée auxquelles nous faisons face en ligne ne sont pas radicalement différentes de ceux de l'ère pré-Internet, et 2) que nous devons reconcevoir près la lecture comme dont une activité les deux humains et algorithmes informatiques sont capables.

John C. Hunter is Associate Professor in Comparative Humanities at Bucknell University, 1 Dent Drive, Lewisburg, PA 17837. Email: jchunter@bucknell.edu

CCSP Press
Scholarly and Research Communication
Volume 5, Issue 2, Article ID 0502152, 10 pages
Journal URL: www.src-online.ca
Received December 12, 2013, Accepted January 11, 2014, Published April 22, 2014

Hunter, John C. (2014). "All data is credit data," or, on close reading as a reciprocal process in digital knowledge environments. *Scholarly and Research Communication,* 5(2): 0502152, 10 pp.

Introduction

> Once I found a beautiful camera phone, lying on the sidewalk. It was muddy and the signal was dead, but I took it home anyway, and the Eves caught me with it. "Don't you know any better?" they said. "Such a thing can hurt you! It can burn your brain! Don't even look at it: if you can see it, it can see you."
>
> —Margaret Atwood, *The Year of the Flood* (2009)

The new knowledge environments of the digital age are often described as places where we are all closely read, with our buying habits, our location, and intimate details of our identities available to advertisers, online merchants, the government, and others through our use of the Internet. This is often represented as an imminent or achieved destruction of privacy in which governments and businesses learn about our activities and desires using means that were unavailable in the pre-digital era (e.g., Andrews, 2012; Lanier, 2012; Mayer-Schönberger, 2011). As Jaron Lanier (2012) puts it (rather apocalyptically) in *You Are Not A Gadget*: "The deep meaning of personhood is being reduced by the illusions of bits. Since people will inexorably be connecting to one another through computers from here on out, we must find an alternative," adding that we should try "to be a person instead of a source of fragments to be exploited by others" (p. 21). Lanier's contrast between "deep" pre-digital selfhood and the supposedly diminished subjectivity manifested on digital networks is common to many articulations of this loss of control. One legal scholar refers to our off-line subjective state as "people's pre-existing autonomy," and the Enlightenment discourse of individual rights that such language evokes is the basis for the privacy rights that are being threatened (Pagallo, 2011; Griffin, 2008). Another, by contrast, refers to our online manifestations as "second selves" or "digital doppelgängers" (Andrews, 2012, p. 45), again insisting on the belatedness and inferiority of our online presence when compared to our "real" material selves. The response to this perceived crisis is to call for more privacy safeguards to be built into search engines, online financial transactions, and the uses of data about individuals by the entities with which we interact (e.g., Pentland, 2009; Froomkin, 2000). More "privacy by design" is needed because "[p]rivacy is not something that appear[s] naturally online, it must be deliberately architected" (Castelluccia, 2012, p. 31; see also Lessig, 2013; Witte, 2013). This is the Internet as a new world, one that resembles a 19th century "Darkest Africa" in that it is both magical and in obvious need of the European Enlightenment model of civilization.

Like nearly all forms of digital exceptionalism, the claim that the crisis of online privacy is totally unprecedented overlooks a dense, complex history that conditions the various responses to our online readability – in this case, a history of making people "readable" via their clothes, behaviour, bodily characteristics, physical locations, language, et cetera – which has coexisted very easily with Modernity's construction of the "private individual" and individual rights. It will be the work of this paper to recall this history of close reading and to analyze how its tropes are being replicated in digital environments.

Whether legally or culturally enforced, attempts to regulate people's behaviour and appearance have always been a feature of Western culture. From ancient Roman restrictions on conspicuous consumption (Dari-Mattiacci & Plisecka, 2012) to early

Hunter, John C. (2014). "All data is credit data," or, on close reading as a reciprocal process in digital knowledge environments. *Scholarly and Research Communication,* 5(2): 0502152, 10 pp.

modern sumptuary laws (Hunt, 1996; Killerby, 2002; Raffield, 2002) and from gendered clothing norms to racial profiling (Meehan & Ponder, 2002), people have always been read and/or judged by their appearance, and have always been conscious of these omnipresent interpretations of their identity. The extensive historicist body of scholarship on performativity has shown how consciously and publicly we perform our gendered, national, sexual, and professional identities (e.g., Butler, 2006; Dent & Whitehead, 2002; Ehlers, 2012; Negra, 2006). And, as Marjorie Garber (among many others) has pointed out, it makes many ordinary people (not just governments and other elites) nervous when the people around them cannot be read and normatively categorized via visual clues (Garber, 1997). However privacy is construed or justified, the idea that we could not be anonymously scrutinized, interpreted, and/or unfairly judged by others prior to the advent of the Internet is risible. The binary opposition between our "real" selves and our online identities outlined above is thus just a lazy unexamined assumption. The question is why theorists of the digital world (like Lanier and Andrews) so often think that they need it – what is driving the urge to bracket our online lives from our "private" lives when life in the West has always been a balance between external forces (seeking to know, circumscribe, and control how we behave) and individual or communitarian responses to these forces?

This article argues that the anxiety about being closely read in networked environments is not a response to a new technological threat, but the articulation of a heretofore impossible desire: the desire to read the world around us without leaving traces or being read in return. As N. Katherine Hayles (among others) has argued, digital technology has radically extended and transformed the concept of what it means to read (Hayles, 2012). The desire to read anonymously, as it were, is a result of a failure to accept the full consequences of this change. It is fostered by our bodily experience of traversing the Internet – because we do not directly experience ourselves being read and interpolated in the ways that occur in any material public setting, we wrongly assume that we are not (and should not) be "seen" online. It is also encouraged by the marketing materials for our networked digital devices, which dwell on our capacity to access data and not on the extent to which we necessarily become nodes in other people's networks by doing so (Rainie & Wellman, 2012).

As strong as this desire may be, however, it is also impossible: it is oblivious of the ways in which being read is a fundamental price for living in communities (as discussed above); it is fundamentally inconsistent with the reciprocal character of networked data environments (Manovich, 2001); and it is an important reason why the online privacy debate has been unable to establish itself properly. Reading (whether one interprets texts, passersby in a street, or social practices) has always been a socially embedded and reciprocal act – this is why one can buy Harry Potter novels with "adult" covers[1] and *Fifty Shades of Grey* novels with anodyne covers[2]; someone may be watching and judging, even as we while away the bus ride to work. The acts of reading that we most resent when they are applied to us in digital knowledge environments (i.e., interpretations of our spending or communication habits) are the products of our participation in networked environments. We need to relearn how the legal presumption of privacy in no way arrests or displaces the kinds of sumptuary, performative, and/or judgmental readings that have always marked social life – even when that life is online.

Close-reading machines

Commercial entities and/or their computers are adept and sensitive close readers of human beings, and the vocabulary and assumptions behind these acts of interpretation are almost identical to those of human literature scholars. Douglas Merrill, the CEO of the online loan company ZestFinance (and a former CIO of Google) describes the act of interpreting people through their online profiles as follows:

> "We feel like all data is credit data, we just don't know how to use it yet," he says. "This is the math we all learned at Google. A page was important for what was on it, but also for how good the grammar was, what the type font was, when it was created or edited. Everything … Data matters. More data is always better" (Hardy, "Just the Facts. Yes, All of Them," 2012, n.p.).

Though Merrill calls it "math," what he is describing here is close reading in terms that any literary critic would recognize. The context for this reading is the decision his company makes about the riskiness of loans to lower-income people who do not have access to the forms of credit that middle and upper class people take for granted. His point is that (in his company's algorithms) a much wider spectrum of textual data is read and interpreted. What Jaron Lanier derided as a "source of fragments" is here proudly and explicitly just that – and the more fragments ZestFinance can find, the more likely they are (so they claim) to make a loan to a credit-worthy person who is NOT read as such by mainstream banks (Hardy, "Big Data for the Poor," 2012). Reading a loan applicant's profile is the product of the same patient and detailed techniques as scholars use to interpret a Web page, a painting, or a novel – they are just performed by algorithms. N. Katherine Hayles has pointed out that the specific differences in these reading environments (print, hypertext, and machine reading) need to be attended to, but she also recognizes and emphasizes the synergistic interactions among the three realms (Hayles, 2010, p. 75ff.). Close reading is thus not something that people do and machines don't (or only do in some perverse, dangerous way); its methods cannot be artificially restricted to certain types of texts and not others. It is the reciprocal process of communication, in material, online, and virtual communities.

In some ways, computers are already better readers than human beings. A recent *Economist* article on the effects of "Big Data" discusses the ability of cloud-based computers to read credit card transaction data and detect fraud: "when the computer looks at all the payments in its system, it is remarkably good at weaving together the bits of information to spot fraud" ("Big Data: Crunching the Numbers," 2013, n.p.). Consciously or not, the writer is alluding to the Latin verb *textere*, meaning "to weave," from which the English word "text" is derived – the computer is weaving a readable text where no unassisted human reader could perceive one. Another banker talks about how his company's computer "raised a red flag even though each payment looked legitimate. 'It saw a pattern when there shouldn't have been a pattern …'" And why is this advance to be celebrated? In commercial terms, because it allows these small banks to issue credit cards and thus regain "a rich source of data on their customers' spending patterns" ("Big Data: Crunching the Numbers," 2013, n.p.). Issuing credit cards allows banks to perform acts of reading that they can monetize, and the article quotes Douglas Merrill of ZestFinance to reinforce this point: "Every bit of data is noise, but when you add enough of them together in a clever way you can make sense of the garbage" (n.p.).

Hunter, John C. (2014). "All data is credit data," or, on close reading as a reciprocal process in digital knowledge environments. *Scholarly and Research Communication,* 5(2): 0502152, 10 pp.

Computers can make interpretable texts out of people as long as they can obtain enough fragments to read, and they do this better than human beings could.

What needs to be stressed is that (motives notwithstanding) this is no different from the ordinary, non-digitally mediated world: when we walk down a street, our conscious affect is blended with what we unconsciously reveal (or suggest) through our clothes and deportment and the prejudices those viewing us use to identify us (rightly or wrongly) in their minds. An enormous body of neuroscientific research has shown how actively and largely unconsciously we interpret every encounter in our lives (e.g., Aarts, Chartrand, Cheng, Custers, Danner, Dik, & Jefferis, 2005; Bargh & Chartrand, 1999; Moskowitz, Newman, & Uleman, 1996). Moving around in the Internet creates the same mixture of conscious and unconscious signals mixed with the prejudices of whomever (or whatever) is interpreting them. Just as our desire for privacy cannot stop us from being interpreted in ways that we can only partially control in our material communities, our online traces can always be read and we will remain oblivious to the motives and misconceptions of these readings.

As the logic of instant knowledge availability gets stretched far beyond search engines, these processes are becoming more automated, with acts of reading being performed on our behalf and brought to our attention via a search engine's interpretation of our desires (or, as with TripAdvisor, aggregated survey responses measuring the satisfaction of others). As Eric Schmidt, the Executive Chairman of Google, put it in a *Wall Street Journal* interview in 2010:

> "We're still happy to be in search, believe me. But one idea is that more and more searches are done on your behalf without you needing to type."
>
> "I actually think most people don't want Google to answer their questions," he elaborates. "They want Google to tell them what they should be doing next."
>
> Let's say you're walking down the street. Because of the info Google has collected about you, "we know roughly who you are, roughly what you care about, roughly who your friends are." Google also knows, to within a foot, where you are. Mr. Schmidt leaves it to a listener to imagine the possibilities: If you need milk and there's a place nearby to get milk, Google will remind you to get milk. It will tell you a store ahead has a collection of horse-racing posters, that a 19th-century murder you've been reading about took place on the next block (Jenkins, 2010).

This process, known as "autonomous searching" or "reality mining," is fundamental to the new Google Glass and is a logical design response to the sheer scope of the data that our personal digital devices are capable of transmitting to users. But it is also the reason we use TripAdvisor – to tell us what we should be doing next. And many of the products being designed for individual consumers to use as they traverse modern life are based on the same assumption that we want to know as much as possible about whatever we choose to look at.

Toyota, for example, is working on an experimental interactive technology called Window to the World, which makes the rear-seat passenger windows of a car into interactive screens that allow one to draw pictures and zoom in and identify/quantify the objects that one sees (Toyota Window to the World, 2011). Clearly intended as a purchase option for families with children, it is a version of augmented reality technology – a landscape that was once passive and unavailable to the car passenger's understanding becomes responsive and open to be known. It is easy to see how it could be extended: towns, farms, and buildings could be named as the car passes them. If facial recognition software was added, even personal identities could be generated, and Window to the World would start to create some of the same ethical dilemmas (and undoubtedly face some of the same legal challenges) as Google Earth cameras (Sheppard & Cizek, 2009; "Privacy Lawsuit Against Google Grows," 2011). More than a symptom of parental willingness to spend a large sum to ensure peace on a cross-country car journey, Window to the World is symptomatic of the ways in which we expect the world to be readable to us – it is not enough to merely spectate, we expect to be able to know and "interact." Notwithstanding this, one could reasonably expect the family represented in Toyota's film reacting in horror if surveillance camera data revealed the precise time and date of their family car's presence in that landscape to a third party. We want the same thing the banks want in issuing credit cards – to know as much as possible in case that knowledge might be useful or materially advantageous to us. And we use exactly the same tools and reading techniques as banks in order to obtain it.

Privacy and interactivity

As long as the online privacy debate refuses to recognize the historical continuities between our online and material lives and the fundamental similarity between private individuals and corporate/institutional readers, it will never be properly grounded. If we look at some of the means individuals use to protect their privacy while transacting their daily business, we find the same reciprocity – the openness of digital media to interpretation from any node in our networks means that the technology we employ to stay private can also be used against us. When the New England Patriots tight end Aaron Hernandez was arrested for murder recently, the *New York Times* described in great detail how the police built their case against him:

> The motive for the killing might have been age-old, but the police used a variety of modern investigative methods and relied on the technology of connected and interactive devices to build their case against Hernandez. Piecing together cellphone tower tracking, text messages and surveillance tapes – including video recorded by 14 cameras trained on the outside and inside of Hernandez's home – the police constructed a timeline and concluded, in the words of McCauley, that Hernandez "orchestrated the execution" of Lloyd, 27 (Pennington, 2013).

The very surveillance cameras that Hernandez purchased to protect his privacy became vital sources of the most potentially devastating information for his very public trial; the SMS messages he sent to allegedly enable a murder are now part of the evidence against him. The police have constructed a complex narrative out of fragmentary pieces from the commonplace technologies of everyday life, and it allows Aaron Hernandez to be interpreted as a suspect in a murder case. It rarely occurs to us that

Hunter, John C. (2014). "All data is credit data," or, on close reading as a reciprocal process in digital knowledge environments. *Scholarly and Research Communication,* 5(2): 0502152, 10 pp.

our networked communication technologies (which are so commonplace as to be invisible) allow us to be read just as effectively as they allow us to direct our lives. The recent revelations made by Julian Assange and Edward Snowden, of course, show how they can work against the state too (Rodriguez, 2013).

The plethora of recording devices that we carry are now often the first sources of information to which the authorities turn in order to solve a crime. In the aftermath of the Boston Marathon bombing, film footage and cellphone camera data were urgently solicited from everyone who had been at the scene because people "don't know that they were witnesses" (Levs, 2013). In this regard, the investigation of the Boston bombing almost exactly mimics the pursuit of the "rogue agent" Aaron Cross in *The Bourne Legacy* (released just eight months before the bombing). For the amoral U.S. government agencies trying to find Aaron Cross, the entire planet is an aggregation of surveillance videos to be read, and understanding Cross's motives is best done by government agents watching video recordings of him as he was transformed from a sad-sack soldier into a physically enhanced government assassin. Other, old-fashioned forms of detection are represented as too risibly slow and inadequate to the task of finding two people among hundreds of millions. Privacy is not just flouted in this film, it is represented as beside the point: we can all be witnesses or targets if we can be framed (literally and metaphorically) as such.

What, then, is the status of privacy in digital knowledge environments? The legal situation in online environments is (in the American context) quite clear, albeit highly unsatisfactory to many (Lee, Rubinstein, & Schwartz, 2008). Our right to data privacy is actually a right to seclusion – a right that we give up when we voluntarily give information about ourselves to a third party:

> Once a person discloses information to a third party, as she does when requesting a URL or when running search queries, she relinquishes any reasonable expectation of constitutional privacy she has in that information. As one of the authors of this essay has noted, information privacy law in the US contains a strand that considers privacy merely as an interest in "data seclusion." Individuals have a right to keep their information secluded, but once they share it with others, privacy rights end. The Supreme Court relies on this paradigm and interprets the Fourth Amendment as protecting only information that has not been shared with others (Rubinstein et al., 2008, p. 273).

This clearly does not explicitly license large-scale data mining such as that performed by the NSA and revealed by Edward Snowden or the more recent revelation of the Drug Enforcement Administration's co-option of AT&T (Nixon, 2013; Moynihan & Shane, 2013) As legal scholars know, however, there is a significant lag between government practice and the regulatory framework:

> In response to the absence of constitutional protections, Congress has enacted an incomplete patchwork of information privacy statutes. For a variety of reasons, the current statutory framework is, by and large, inadequate to protect privacy against the growing availability of personal information. As a consequence, information possessed by third parties, such as search engines and

> ISPs, can be acquired by the government through subpoenas or court orders that do not carry with them the same judicial oversight, or require the same level of particularized suspicion, that the law prescribes for warrants (Rubinstein et al., 2008, p. 274)

The state is literally overseeing us in ways that it has always done, and as such it is doing no more than using the means of reading that are available to it. It may be that it was always already sinister and intolerable – but it is a fundamental mistake to imagine that what the NSA and other agencies are doing is something new or unprecedented.

This is absolutely NOT to recommend quietism or resignation in the face of what is happening. In order to renegotiate how the information that exists about us in digital networks is used, however, we need to start from two new bases. The first is the recognition that the Internet is not a completely new world; it is an arena for social interpretation, control, and resistance that works just like the *agora* of ancient Athens or the student culture of any high school, and the sooner we recognize this and apply what we know about socially grounded acts of reading to it the better. The second is the acceptance that digitally networked data is by its nature shared and interpretable from several nodes in the network. We cannot arbitrarily limit how and when we are interpreted.

Notes

1. See http://www.amazon.co.uk/Harry-Potter-Adult-Covers/lm/2VELABIR01VON [September 3, 2013].

2. See http://www.hollywood.com/news/celebrities/35224898/fifty-shades-of-grey-disguise-your-copy-with-these-book-covers [September 5, 2013].

References

Aarts, H., Chartrand, T.L., Custers, R., Danner, U., Dik, G., Jefferis, V.E., & Cheng, C.M. (2005). Social stereotypes and automatic goal pursuit. *Social Cognition, 23*(6), 465–490.

Andrews, Lori. (2012). *I know who you are and I saw what you did: Social networks and the death of privacy*. New York, NY: Free Press.

Bargh, John A., & Chartrand, Tanya L. (1999). The Unbearable automaticity of being. *American Psychologist, 54*(7), 462–479.

Big data – crunching the numbers. (2013, June 24). *The Economist*, Special Report on International Banking. URL: http://www.economist.com/node/21554743 [August 21, 2013].

Butler, Judith. (2006). *Gender trouble: Feminism and the subversion of identity*. New York, NY: Routledge.

Castelluccia, Claude. (2012). Behavioural tracking on the Internet – A technical perspective. In Serge Gutwirth, Ronald Leenes, Paul De Hert, & Yves Poullet (Eds.), *European data protection: In good health*? (pp. 21–33). New York**,** NY: Springer.

Dari-Mattiacci, Giuseppe, & Plisecka, Anna E. (2012). Luxury in ancient Rome. An economic analysis of the scope, timing and enforcement of sumptuary laws. *Legal Roots,* 1, 189–217.

Dent, Mike, & Whitehead, Stephen. (2002). *Managing professional identities: Knowledge, performativity, and the "new" professional*. New York, NY: Routledge.

Ehlers, Nadine. (2012). *Racial imperatives: Discipline, performativity, and struggles against subjection*. Bloomington, IN: University of Indiana Press.

Froomkin, A. Michael. (2000). The death of privacy? *Stanford Law Review*, *52*(5), 1461–1543.

Garber, Marjorie. (1997). *Vested interests: Cross-dressing and cultural anxiety*. New York, NY: Routledge.

Gilroy, Tony. (2012). *The Bourne legacy*. Universal Home Entertainment.

Griffin, James. (2008). *On human rights*. Oxford: Oxford University Press.

Hardy, Quentin. (2012, March 24). Just the facts. Yes, all of them. *New York Times.* URL: http://www.nytimes.com/2012/03/25/business/factuals-gil-elbaz-wants-to-gather-the-data-universe.html [August 3, 2013].

Hardy, Quentin. (2012, July 5). Big Data for the Poor. *New York Times.* URL: http://bits.blogs.nytimes.com/2012/07/05/big-data-for-the-poor [August 13, 2013].

Hayles, N. Katherine. (2010). How we read: Close, hyper, machine. *ADE Bulletin* 150, 62–79.

Hayles, N. Katherine. (2012). How we think: Transforming power and digital technologies. In David M. Berry (Ed.), *Understanding digital humanities* (pp. 42–67). New York, NY: Palgrave Macmillan.

Hunt, Alan. (1996). *Governance of the consuming passions: A history of sumptuary law*. London: Palgrave Macmillan.

Jenkins, Jr., Holman W. (2010, August 14). Google and the search for the future. *Wall Street Journal.* URL: http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html [August 3, 2013].

Killerby, Catherine Kovesi. (2002). *Sumptuary law in Italy 1200 – 1500*. Oxford: Oxford University Press.

Lanier, Jaron. (2012). *You are not a gadget: A manifesto.* New York, NY: Vintage.

Lessig, Lawrence. (2013, June 12). It's time to rewrite the Internet to give us better privacy and security. *The Daily Beast*. URL: http://www.thedailybeast.com/articles/2013/06/12/it-s-time-to-rewrite-the-internet-to-give-us-better-privacy-and-security.html [July 13, 2013].

Manovich, Lev. (2001). *The language of new media*. Cambridge, MA: MIT Press.

Mayer-Schönberger, Viktor. (2011). *Delete: the virtue of forgetting in the digital age.* Princeton, NJ: Princeton University Press.

Meehan, Albert J., & Ponder, Michael C. (2002). Race and place: the ecology of racial profiling African American motorists. *Justice Quarterly, 19*(3), 399–430.

Negra, Diane. (2006). *The Irish in us: Irishness, performativity, and popular culture.* Durham, NC: Duke University Press.

Nixon, Ron. (2013, July 3). U.S. Postal Service logging all mail for law enforcement. *New York Times.* URL: http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html [August 4, 2013].

Pagallo, Ugo. (2011). Designing data protection safeguards ethically. *Information 2*(2), 247–265.

Pennington, Bill. (2013, June 26). Former Patriots tight end is charged with murder. *New York Times.* URL: http://www.nytimes.com/foootball/patriots-aaron-hernandez-arrested.html [July 18, 2013].

Pentland, Alex. (2009). Reality mining of mobile communications: Toward a new deal on data. In Soumittra Dutta and Irene Mia (Eds.), *The Global Information Technology Report 2008–09* (pp. 75–80). Davos: World Economic Forum.

Privacy lawsuit against Google grows. (2011). *UPI.* URL: http://www.upi.com/Business_News/2011/07/14/Privacy-lawsuit-against-Google-grows/UPI-59711310676116 [August 4, 2013].

Raffield, Paul. (2002). Reformation, regulation, and the image: Sumptuary legislation and the subject of law. *Law and Critique,* 13, 137–150.

Rainie, Lee, & Wellman, Barry. (2012). *Networked: the new social operating system*. Cambridge, MA: MIT Press.

Rodriguez, Gabriel. (2013). Edward Snowden interview transcript FULL TEXT: Read the *Guardian's* entire interview with the man who leaked PRISM." *PolicyMic*. URL: http://www.policymic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism [July 18, 2013].

Rubinstein, Ira S., Lee, R.D., & Schwartz, P.M. (2008). Data mining and Internet profiling: Emerging regulatory and technological approaches. *University of Chicago Law Review, 75*, 261–285.

Shane, Scott, & Moynihan, Colin. (2013, September 1). Drug agents use vast phone trove, eclipsing NSA's. *New York Times*. URL: http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html [September 2, 2013].

Sheppard, Stephen R.J., & Cizek, Petr. (2009). The ethics of Google Earth: Crossing thresholds from spatial data to landscape visualisation. *Journal of Environmental Management, 90*(6), 2102–2117.

Smith, Matt, & Levs, Josh. (2013, April 15). FBI will try to rebuild Boston bombs. *CNN*. URL: http://www.cnn.com/2013/04/15/us/boston-marathon-investigation/index.html [April 19, 2013].

Toyota Window to the World. (2011). *YouTube*. URL: http://www.youtube.com/watch?v=dl9eqdZpvJU [September 29, 2013].

Uleman, J.S., Newman, L.S., & Moskowitz, G.B. (1996). People as flexible interpreters: Evidence and issues from spontaneous trait inference. In M.P. Zanna (Ed.), *Advances in experimental social psychology*, 28, pp. 211–279. New York, NY: Academic Press.

Witte, Derek. (2013). Bleeding data in a pool of sharks: the anathema of privacy in a world of digital sharing and electronic discovery. *South Carolina Law Review, 64*, 717–753.

Hunter, John C. (2014). "All data is credit data," or, on close reading as a reciprocal process in digital knowledge environments. *Scholarly and Research Communication, 5*(2): 0502152, 10 pp.