The Political Economy of Communication
1(2), 89–94

http://www.polecom.org

Uncovering the data panopticon: The urgent need for critical scholarship in an era of corporate and government surveillance

John L. Sullivan, *Muhlenberg College*

Big data and the panoptic sort

In Philip K. Dick's 1956 science fiction short story, *The Minority Report*, crime in a futuristic United States has been all but extinguished because the police have discovered the ability to predict future events. In this peaceful dystopia, suspects are arrested and charged before their crimes are even committed. While real-world law enforcement agencies cannot (yet) predict future events, the recent revelations about the scope and nature of the National Security Agency's (NSA) domestic digital spying program suggest they have developed some formidable tools to locate would-be terrorists. Privacy advocates were outraged by whistleblower Edward Snowden's revelation that the NSA, in cooperation with technology companies, routinely stored, processed and analyzed millions of private emails, video chats, online phone calls, and internet file transfers under the auspices of a program called PRISM. Recent news reports based upon Snowden's documents have revealed that even encrypted emails, documents, and online banking transactions are being regularly accessed by the NSA (Larson and Shane, 2013).

While these revelations about domestic digital wiretapping without court orders have caused a stir in the American and global press, the privacy dangers associated with this type of data surveillance are not new to the scholarly community. Exactly 20 years ago, communication scholar Oscar H Gandy Jr (1993) meticulously outlined the growing threat to individual privacy posed by the cooperation between corporate and government data gathering in a book called *The Panoptic Sort*. At a time when the internet was in its infancy, when desktop computer processing was a fraction of what it is today, and five years before the founding of Google, Gandy warned that organizations like Equifax, TRW, and the Direct Marketing Association (DMA) were amassing huge repositories of consumer data that were gathered passively whenever individuals made purchases via credit cards. When these data are combined with sophisticated matching algorithms and sorted against huge government databases like the census, he argued, they enabled precise tracking of individuals' behaviors, political views, and other sensitive private information. The precision of such discrimination transforms the routine sorting of personal data into a powerful form of institutional power. Building upon Foucault's (1995) seminal analysis of disciplinary systems in society, Gandy argued that the scale of the data collection and analysis performed by government and corporate institutions created a panopticon wherein citizen actions would eventually become

circumscribed within an ever-widening net of personal data surveillance. The end result, he observed, is "an antidemocratic system of control that cannot be transformed because it can serve no purpose other than that for which it was designed—the rationalization and control of human existence" (Gandy, 1993: 227).

We've come a long way since 1993. Who could have imagined services like Facebook, Twitter, and Tumblr that not only encourage, but actively incentivize the voluntary dissemination of personal information online? Over the past 20 years, the centrality of the internet to the global communications infrastructure has made it a target for the type of panoptic sorting that Gandy described. Now that the world knows about PRISM, it is tempting to imagine that enhanced public scrutiny will effectively limit these programs. I don't think that is likely. In fact, there are four specific trends that foretell a greater *expansion* of the data panopticon:

- convergence and the central place of software in social, commercial and political systems;
- the growing importance of metadata for routing, storage and sorting of information;
- the global business of data storage and retrieval;
- the blurring of lines between corporate and government data mining.

The convergence of digital technologies and the importance of software

In the previous era of analog technologies, such as wired telephones and reel-to-reel tapes, each specific technology had a limited range of capabilities alongside a specific set of legal standards to accompany their use. The Wiretap Act of 1968, for example, prohibits law enforcement from wiretapping telephones without a court order because doing so would violate the 4th Amendment protections of both the suspect and anyone that communicates with them. Today, there are few discrete technologies anymore. Thanks to technological convergence, almost all forms of communication today utilize some form of digital communication, and many do this via the Internet. Software has now replaced specific forms of communication hardware as the nexus for new types of digital communication, from Skype and FaceTime to emails and tweets. Creating legal precedents for protecting individual privacy throughout this myriad of new options has been difficult. Indeed, new options are emerging all the time, and software is extremely fungible in functionality as it adapts quickly to new situations and uses. We lack a coherent legal regime to counteract the interception of these communications. For example, Skype phone calls can be protected under the existing federal wiretap laws, but emails and text messages cannot.

The rise of metadata

The expansion of online communications has generated an explosion of metadata. Metadata are the transaction records that are generated whenever you send an email or text message. It identifies the location from which the message was sent, when it was sent, the subject of the message, the recipient(s) of the message, the web address of the recipient(s), and more. The Obama Administration has argued that its domestic intelligence program complied with the law because it simply scanned the metadata of email transactions to search for anomalies rather than accessing the content of those emails. As a recent article in *The Economist* (2013) pointed out, however, while the usefulness of metadata in an analog era was limited (hence the lower evidentiary standards required in courts to obtain that information), today, thanks to the internet, "metadata can now provide a

detailed portrait of who people know, where they go, and their daily routines." (para. 8) Therefore, the argument that random metadata searches do not violate users' privacy becomes difficult to sustain.

The business of data storage and retrieval

The cost of storing digital data has fallen dramatically in the past 20 years, making the retention of vast quantities of individual data routine and cheap. This incentivizes the retention of digital information in 'the cloud' for longer periods of time. This creates a valuable resource for commercial data miners and law enforcement officials alike. As *Wired Magazine* (Copeland, 2013) outlined in its 20th anniversary edition, in 1993 a gigabyte of computer hard drive space cost almost $1,900.00; today the same amount of digital storage space is worth four cents. This dramatic drop in the cost of storage naturally encourages the retention of digital information by companies and the government. This raises important privacy concerns. Mobile telephone providers, such as Verizon, AT&T, and T-Mobile, regularly store customer metadata (the records of all their telephone communications, including location information) for 18–24 months depending on the carrier. Companies like Google and Dropbox offer generous amounts of online data storage ('cloud computing') to users in exchange for the ability to target those consumers with advertising and marketing messages. Companies like Facebook and Twitter profit handsomely by mining their massive storehouses of user data for the purposes of target marketing to specific users.

The blurred line between corporate and government data mining

Lastly, the Snowden leaks have revealed that the wall between corporate and government data mining is paper thin. Since the revelations about the NSA became public, technology companies like Apple and Google have publicized the fact that they have received thousands of NSA requests for individual user data over the past 12 months. While some companies have resisted handing over user data without a specific warrant from the government, other technology companies have complied without challenge, worried about the implication of refusing the federal government. Additionally, as a headline article in *The New York Times* (Sengupta, 2013) outlined, the NSA and FBI have, increasingly, routinely analyzed huge databases of online communications. They have signed lucrative contracts with Silicon Valley technology companies to perform these analyses. *The New York Times* also uncovered the existence of a revolving door between technology companies and the government. For example, former Facebook Chief Security Officer Max Kelly was hired by the NSA in 2010 (Risen and Wingfield, 2013). Such arrangements create a clear conflict of interest for the companies to whom we have entrusted our data. For the first time, these companies may have both a legal and *financial* interest in handing over sensitive personal information to government agencies. Of all of the recent revelations about the mining of individual data, this one is perhaps the most troubling.

What's the harm?

Given these threats to individual privacy online, what's the harm if programs like PRISM have been effective in thwarting potential terrorist attacks? Snowden answered this question himself in his infamous interview with *The Guardian* newspaper (Greenwald, 2013) by saying:

> Because even if you're not doing anything wrong you're being watched and recorded. And the storage capability of these systems increases every year consistently by orders of magnitude to where it's getting to the point where you don't have to have done anything wrong. You simply have to eventually fall under suspicion from somebody even by a wrong call. (7:14–7:33)

Snowden is alluding here to the problem of 'collateral damage' arising from the search of online personal data. Innocent citizens may be caught up in data searches that are meant to locate illegal activities. This problem was most recently demonstrated in 2012 when a warrant to search the email account of Paula Broadwell for a harassment charge unwittingly uncovered an extramarital affair between her and David Petraeus, the then CIA Director and former General. These targeted searches also reverse the burden of proof. Once someone is targeted for government scrutiny because of an email they may have sent, it becomes difficult for them to clear their name.

Additionally, we may have started down a path that will be difficult to alter. Once companies and governments begin collecting and storing citizens' private data, those institutions will continue to imagine new uses for such data, if only to justify the expense of gathering and storing it. History and human nature tell us that the storage and sorting of online personal data will increasingly become the solution to problems we haven't even yet encountered, alongside existing problems (tracking terrorists, criminals, tax evaders, copyright violators, etc.)

The public and the role of critical scholarship

Given that we still live in a liberal democracy, what is the public's role in this process? Shouldn't citizens help to shape a proper balance between privacy and security? In *The Panoptic Sort*, Gandy traced the social origins of privacy and considered the available cognitive strategies for a public trying to grapple with this amorphous concept within a changing techno-cultural environment. In focus group interviews, Gandy explored the types of information consumers had about the technologies that could be used to observe and profile them. Respondents were asked whether they thought these practices were legitimate, and whether they had reflected upon the sharing of private information among interested parties (including sharing between private corporations and government agencies). These 1992 focus group participants were quite sophisticated in their responses, observing that the gathering of personal information may be justified or even beneficial in some cases, but that no information "should ever be used to restrict or limit one's pursuits, happiness, or joy of life" (Gandy, 1993: 135). Gandy also cited nationwide polling conducted in 1990 by Equifax, which found that 46 percent of respondents were "very concerned" about "threats to... their personal privacy" (Gandy, 1993: 140). Today, in a post-September 11 society, the surreptitious gathering of personal information has reached new heights, yet public opinion on the appropriate boundaries of private information retrieval has shifted markedly. A recent poll conducted by the Pew Research Center, for example, found that 56 percent of Americans approve of the NSA's tracking of phone records as an acceptable method of combatting terrorism (Pew Research Center, 2013). In that same poll, respondents were almost equally divided about the NSA's policy of scanning all emails to prevent terrorism; 52 percent disapproved while 45 percent approved.

We see a somewhat disturbing trend here. While the tools available to gather, store and process personal information have dramatically expanded in the past 20 years, the public's privacy concerns

seem to have abated, albeit only slightly. Increased terrorism fears are no doubt one of the prime catalysts for this, but we should not discount the prospect that popularization of email, search engines like Google and social media have lessened our inhibitions regarding the sharing and monitoring of personal information. As Mark Andrejevic (2005, 2007, 2009) has noted in his impressive corpus of research, citizens are not only being continually monitored by corporations and law enforcement, they are essentially monitoring each other. This is what he calls 'lateral surveillance'. At a time when we are encouraged to continually monitor our friends, relatives, neighbors and acquaintances via social networking, the legitimate boundaries surrounding our private information have been blurred.

As Snowden's startling NSA revelations demonstrate, shifts in the nature of digital privacy require a vigorous response from critical scholars. Following Gandy's 1993 book, there needs to be more research on the political economy of personal data gathering, storage and analysis. Rather than accept these new technological systems as a starting point for analysis, we should question the philosophical and institutional foundations of the modern surveillance state. As Gandy noted in his conclusion, we should not jump on the metaphorical train to the future without first addressing its path and destination. He wrote:

> It is the work of critical scholarship to raise doubts in the minds of the other passengers, to give voice to their unspoken concerns about the competence of the engineers, to validate their mistrust of the digitized voices that announce the next station or the final destination. It is the work of critical scholarship to speak to the engineers, to wonder aloud with them about whether the tracks will carry a train this long, this fast, that far. (Gandy, 1993: 230)

Along with a greater awareness of the personal data industry and the hand-in-glove cooperation among technology companies, law enforcement authorities, and intelligence agencies, we need to provide mechanisms for the public to guide policymakers about the appropriate parameters of online surveillance. For example, to what extent are we willing to accept online surveillance in the service of public safety? For public discussion to occur, we need more transparency from both corporations and the government about the ways in which our data are gathered, stored, and searched. Without this transparency, we will be living in a data panopticon with little chance for escape.

Author Bio

John L. Sullivan is Associate Professor of Media and Communication at Muhlenberg College in Allentown, PA. He received his Master's and Ph.D. degrees in Communication from the Annenberg School for Communication at the University of Pennsylvania. His research interests include media industries and the institutional construction of audiences; the political economy of cultural production; the political economy of free, open source software (FOSS) movements; the history of cultural production studies; the historiography of mass communication; and U.S. media policy implementation. He is the author of *Media Audiences: Effects, Users, Institutions and Power* (Sage, 2013).

References

Andrejevic, M (2005) The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society* 2(4): 479–497.

Andrejevic, M (2007) *iSpy: Surveillance and power in the interactive era*. Lawrence, KA: University Press of Kansas.

Andrejevic, M (2009) Privacy, exploitation, and the digital enclosure. *Amsterdam Law Forum* 1(4): 47–62.

Copeland, MV (2013) WIRED 20th anniversary: Storage. *Wired Magazine,* 16 April. Available at: http://www.wired.com/magazine/wired-20th-anniversary/

Foucault, M (1995) *Discipline and punish: The birth of the prison.* 2nd Edition. New York: Vintage Books.

Gandy, OH (1993) *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview Press.

Greenwald G (2013) NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' – video. [Video interview] *The Guardian,* 9 June. Available at: http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

Larson, NP & Shane, S (2013) N.S.A. able to foil basic safeguards of privacy on web. *The New York Times,* 5 September. Available at: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

Pew Research Center (2013) *Public says investigate terrorism, even if it intrudes on privacy: Majority views NSA phone tracking as acceptable anti-terror tactic*. Report: Pew Research Center for the People & the Press, Washington, DC. Available at: http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

Risen, J & Wingfield, N (2013). Web's reach binds N.S.A. and Silicon Valley leaders. *The New York Times,* 19 June. Available at: https://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html

Sengupta, S (2013) The Pentagon as Silicon Valley's incubator. *The New York Times*, 22 August. Available at: http://www.nytimes.com/2013/08/23/technology/the-pentagon-as-start-up-incubator.html

The Economist (2013) Surveillance: Look who's listening. *The Economist*, 15 June. Available at: http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will/print