The Political Economy of Communication
4(2), 18–33

http://www.polecom.org

# Panoptic Missorts and the Hegemony of U.S. Data Privacy Policy

**Jeffrey Layne Blevins**, University of Cincinnati

**Keywords:** Big data, political economy, privacy, hegemony

## Abstract

The amount and scope of data mining practices from our online activities and personal digital media devices should yield highly detailed profiles of our individual preferences, so that marketers can create decidedly calculated and targeted advertising messages. Oscar Gandy described an early version of this process in his 1993 book, The Panoptic Sort: A Political Economy of Personal Information, and critiqued some of its ill effects. This analysis reexamines Gandy's critique and explores further concerns about the panoptic machine, including the 'missort' of personal information and the misrepresentation of individuals. This political economic analysis shows the inability of U.S. privacy policy to properly address the harms of missorting, and examines the hegemonic nature of 'big data' ownership and control.

Personal digital media devices, such as iPads, androids, iPhones and tablets engage and record just about every moment of our social lives. They have the potential to describe the interests, desires, fears, health and well-being of a single individual. Data miners collect and categorise information from our email, search engines, web browsing, and social media apps. They know a lot about who our friends and associates are, where we go, and what we do. All of this digital data collection should allow marketers to make extremely calculated inferences about what we will purchase and to deliver targeted messages accordingly.

As reported in a National Science Foundation White Paper for Privacy in an Era of Big Data Workshop (2015), corporations are able to "collect, store and analyse . . . data to obtain unprecedented insights into consumer behavior and people's activities and habits." For instance, Experian Marketing Services (2014) boasts that its Mosaic USA "is a household-based consumer based lifestyle segmentation system that classifies all U.S. households and neighborhoods into 71 unique segments and 19 overarching groups, providing a 360-degree view of consumers' choices,

preferences and habits." Experian's 19 principal groups range from "Power Elite" and "Thriving Boomers" to "Singles and Starters" and "Economic Challenges". The 71 segments include monikers such as "Kids and Cabernet," "Full Pockets, Empty Nests," "Small Town, Shallow Pockets" and "Urban Survivors" (Experian Marketing Services, 2014).

In the early dawn of the digital media era, Oscar Gandy referred to this kind of data gathering and segmentation in his 1993 book as "the panoptic sort" whereby individuals are sorted according to their political and economic value. In Gandy's view, applying a traditional Marxist critique, the panoptic sort is a technology of power as it identifies, classifies and makes assessments while robbing consumers of the surplus value that is generated by their personal information. The analysis to be presented here will reexamine Gandy's work in the context of the current digital media environment. Of particular importance is his concern that the panoptic sort is devoid of contextualisation and reproduces biases along the lines of race, gender, age, class, and culture.

As noted in a *New York Times* report on the digital collection of personal data: "even as millions of people embrace these data-driven services, many are mistrustful of the kinds of inferences that companies might make based on information gathered about them" (Singer, 2015). While individuals may be uneasy about any inferences about them that are drawn from the collection and aggregation of their personal data – accurate or not – this analysis will focus on another concern. The process of digital media surveillance and data crunching may sometimes misrepresent individuals, resulting in discriminatory and exploitative effects with little to no accountability imposed on the aggregators and distributors of the information. As this political-economic analysis will show, the patchwork of laws and policies in the U.S. that address online privacy miss some of the most serious concerns about big data collection. These are the misrepresentation of individuals and their lack of power in seeking redress for missorting, and the corporate control over personal information. A more comprehensive policy approach to informational privacy is needed to ensure fairness and protect the rights of everyone in the digital age.

## Conceptual frameworks for panoptic sorts and missorts

Gandy's (1993: 1) description of the "panoptic sort" grew out of a project of critical theory about the credit authorisation process and personal data privacy. He found a "discriminatory process that sorts individuals on the basis of their estimated value or worth . . . and reaches into every aspect of individuals lives in their roles as citizens, employees and consumers." Gandy (1993) referred to this process as the "panoptic sort," which he characterised as

> the all-seeing eye of the difference machine that guides the global capitalist system . . . a kind of high-tech, cybernetic triage through which individuals and groups of people are being sorted according to their presumed economic or political value (1).

In Gandy's analysis, one of the most distressing concerns presented by the panoptic sort was its discriminatory impact on the poor and non-whites.

The kinds of concerns presented by the panoptic sort are now often discussed within the nomenclature of 'big data'. This has to do with the management, governance and social impact connected to "the continuous gathering and analysis of dynamically collected, individual-level data about what people are, do and say" (Couldry and Powell, 2014: 1). Recent critical inquiry into the role of big data has explored cultural awareness about the systems of personal data collection and classification. Couldry and Powell (2014) have suggested that even if individuals "are not privy to

the details of when, by whom, and how they have been classified" (2) they are at least aware that this kind of process has occurred. Nonetheless, Couldry and Powell (2014) contend that more transparency and accountability is needed within data collection practices; and they are skeptical about whether or not notions of 'algorithmic power' can properly address critical concerns about the governance of big data collection.

To the contrary, Lash (2007) has gone so far as to argue that 'algorithmic power' has diminished the relevance of hegemony as a core concept of cultural studies in the current era of big data. The concept of hegemony, as defined by Antonio Gramsci (1996) can be employed to analyse the exercise of corporate power through commercial media systems in capitalist societies (see Blevins, 2001: 141-142). In this sense, corporate hegemony is maintained through the state's regulatory apparatuses and civil society acceptance. However, according to Lash (2007), "algorithmic" rules mediate capitalistic power through creation and discovery within a decentralised network as they are

> more and more pervasive in our social and cultural life of the post-hegemonic order. They do not merely open up opportunity for invention, however. They are also pathways through which capitalist power works, in, for example, biotechnology companies and software giants more generally. Power through the algorithm is increasingly important for media companies in digital rights management. A society of ubiquitous media means a society in which power is increasingly in the algorithm (70-71).

Thus, Lash (2007) seems to suggest that algorithms are, perhaps, a form of neutral power; and concludes that "[a]fter hegemony and the meltdown of the classic institutions and their regime of representation, politics leaks out" (5).

However, Lash's (2007) analysis does not seem to consider that media institutions may represent human subjects in new digital forms – through codes and algorithms; and that classic forms of institutional power (such as governmental laws), can protect media companies in significant ways. Furthermore, while algorithms may tell a story based on a set of facts, those facts may lack proper context, may involve incomplete or missing data, and might misrepresent its human subjects in ways that distort, embellish, or otherwise cast them in a false light.

A national survey by Turow, Hennessey and Draper (2015: 4) indicates that a majority of "Americans feel resigned to the inevitability of surveillance and the power of marketers to harvest their data" (4). This is counter to the idea that people fully consent to data gathering as a tradeoff for commercial benefits, such as free or enhanced online services. As Turow, Hennessey and Draper (2015) explain: "[r]esignation occurs when a person believes an undesirable outcome is inevitable and feels powerless to stop it. Rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them" (3). That people are not actively consenting to the unrestricted use of their personal data, but are merely resigned to the occurrence of this phenomenon, raises critical questions about meaningful avenues of resistance and the effectiveness of U.S. data privacy policy. Thus, in contrast to Lash's position, notions of hegemony and how power operates between big data and privacy law are ripe for further political-economic inquiry (especially in regard to struggle over access, accuracy and control of personal data collected via digital media platforms).

In response to Lash's (2007) post-hegemonic notion, Beer (2009) indicated that there is still more to understand about how power operates in the algorithms of digitally mediated platforms:

> The movement toward what is often described as Web 2.0 is usually understood as a large-scale shift toward a participatory and collaborative version of the web, where users are able to get involved and create content. As things stand we have so far had little opportunity to explore how new forms of power play out in this context of apparent 'empowerment' and 'democratisation' (985).

To this end, Couldry and Powell (2014) noted that "as political-economic analyses have developed, we are beginning to see how such shifts have also led to the production of data replacing the production of audiences" (3). Thus, "the exemplary product of mass self-communication is data" and "[i]n the mass self-communication model individuals are still part of an aggregate product to be sold . . . it is their individual acts of communication that compromise the 'Big Data' and drive much media value-extraction" (Couldry and Powell, 2014: 3).

Some of the largest data brokers in the U.S. are Acxiom, Epsilon, TransUnion, Datalogix, Dataium, and Spokeo (U.S. Senate Report, 2013). According to a 2015 IBM study these brokers and others collected over 2.5 quintillion bytes of data per day. Through the assembly of data, these brokers make inferences about such things as religion, political affiliation, medical history, income, and sexual orientation. For instance, Statlistics, advertises a list of Gay and Lesbian adults (see http://www.statlistics.com); Response Solutions markets a list of people suffering from bipolar disorder (http://www.responsesolutionsllc.com); Paramount Media sells lists of people with alcohol, gambling and sexual addictions, and people who are looking to get out of debt (http://www.paramountmediagroup.com); Exact Data lists people who have sexually transmitted diseases, as well as people who have purchased adult material (http://www.consumerbase.com/index.html). Given this scope and scale, political-economic analyses should also be concerned with whether the data (or surplus value extracted from individual acts of communication) potentially produce inaccurate assessments of cultural activity.

It is evident that corporate brokers are collecting a vast amount of data from our daily communication activities. It is less clear how that data is being used, whether it is accurate, credible and representative of who individuals are, what they want and what they will do. Algorithms may tell a story based on a certain set of facts, but these may be incomplete or lack proper context, which raises concerns about how these data may be used to make decisions that affect our economic and social life.

Turow, Hennessey and Draper (2015) describe "the discriminatory potential that seemingly benign pieces of data can have on the opportunities people can have in the public sphere" (20). For example,

> companies may well merge the category "sports fan" with dozens of other characteristics about an individuals' eating habits (at the ballpark, for example), income, number and age of children, house value, vacation habits, mobile-tracked locations, clothes-shopping habits, and media-use patterns to create profiles that dub them winners or losers regarding certain areas of shopping and the advertisements related to them. For reasons they don't understand, people may see patterns of discounts that suggest they are being siloed [sic] into certain lifestyle segments. Certain advertisers may support their media habits but not, perhaps, to the extent that advertisers support neighbors or co-workers. The individuals will vaguely understand that their profiles are the cause, and they may try to change their behavior to get better deals, often without success, all the while wondering why "the system"—the opaque under-the-hood predictive analytics regimes that they know are tracking their lives but

> to which they have no access—is treating them that way (Turow, Hennessey and Draper, 2015: 20).

The scope and scale of big data collection has raised concerns about personal privacy, and the lack of regulatory oversight.

However, privacy concerns are often, and too easily brushed aside as a false dichotomy between "progressive policies that unleash the power of big data and retrograde approaches that lock it up" (Mosco, 2014: 108). A World Economic Forum Report by Dutta and Bilbao-Osorio (2012) championed the economic benefits of the big data industry. They estimated billions in revenue gains from personal location data alone and predicted that even more was to come from retail and social media data. Apart from predicting consumer preference and behavior, "Big Data finds application in new areas such as social media, healthcare, insurance, genetics, and even crime prevention" (National Science Foundation, 2015). All of this may sound like Philip K. Dick's (1956) science fiction short story, *The Minority Report* in which the government uses mutant beings with supposed precognitive power to predict criminal events, so that police can act before they occur. Similarly, the algorithmic formulas that technology and software companies use to surveil our digital media activities try to predict our behavior and sort us into neatly packaged socio-economic silos (Gandy, 1993). This raises critical political-economic questions about the ownership and control of personal data in the digital age.

Moreover, the application of a political economy framework for analysis allows us to assess how missorting is embedded within a system of relationships that allows corporations to assume ownership and control over personal data. There are few forms of redress for the subjects of panoptic surveillance, and little supervision from state regulatory apparatuses. To more fully articulate the relationships of power involving consumers of digital media, corporate owners and regulatory agencies it is necessary to understand that big data is a product of labor. As Fuchs (2013: 20) explained,

> if the commodity of internet platforms is user data, then the process of creating this data must be considered to be value-generating labour. Consequently, this type of internet usage is productive consumption or prosumption in the sense that it creates value and a commodity that is sold. . . . Digital labour creates the internet prosumer commodity that is sold by internet platforms to advertising clients. They in return present targeted ads to users.

In this sense, consumers are the creators of their personal data through the labor of consumption activity. However, we may reasonably consider individuals' lack of power to control the use and application of their own work product. It appears that corporate entities appropriate the surplus value of that labor through the economic base of the digital platforms they own and that power is legitimated through the superstructure of media policies premised on industry self-regulation, and a culture of corporate speech rights.

## A political-economic analysis of digital media privacy

There has been growing concern among political economists about the lack of regulatory oversight in regard to the small number of powerful data brokers. As Mosco (2014) notes, scholarly attention is starting to focus on a handful of companies, including Amazon, Apple, Facebook, Google and Microsoft that have dominated the primary venues for the flow of big data and have become an

integral part of the contemporary political economy. Vincent Mosco (2014) considers the cultural implications arising from the corporate collection and analysis of big data, and notes the difficulties of trying to simplify the complexities of social life through algorithms. Mosco (2014) argues that "panoptic knowledge" doubly created by ubiquitous information and surveillance, fused knowledge and power together, and suggests that: "the key ontological tension is not between knowledge and data, but rather between reason and rhetoric" (212).

The analysis presented here advances this suggestion by exploring U.S. media privacy policy in regard to the tension between data based knowledge (information) and wisdom (understanding and control of that knowledge). While media political economists have explored how the big data crunch of our media consumption activities generates surplus value (see Fuchs, 2013), the missorts of that data and the capacity of U.S. privacy policy to address this problem has received little scholarly attention. As I will show, far reaching arguments for applying First Amendment protection and for industry self-regulation have undercut policy attempts to mitigate inaccurate or discriminatory representation of individuals through big data.

This study applies the moral-philosophical outlook of political economy (as described by Meehan, Mosco and Wasko, 1993) to evaluate contemporary policymaking activities around media privacy and examines how the broad principles of free expression and neoliberal economic theory have been used to justify data mining practices within the law.

The application of a political economy perspective to a legal concern allows us to assess moral accountability and to determine culpability for the ill effects of panoptic sorting. While some industries have codes of ethics and professional councils that monitor and evaluate business practice, it is state apparatuses (through regulation, administrative rulemaking and civil action) that are usually able to exercise authority over corporate activity. However, as this study will show, legislators, administrative agencies and the courts have been less effective in enforcing privacy standards in cyberspace due to the commercialisation and privatisation of data mining activities. As Mosco (2009) explains, "[d]igital systems measure and monitor precisely each information transaction" (137), and then repackage and sell that information. Turning media audiences into a commodity creates conflicting interests among media users, service providers, and the government, particularly in western societies that tend to be more "ideologically committed to private control over economic activity" (Mosco, 2009: 177). In such a neoliberal economic environment, government oversight of commercial transactions of data across private networks is likely to be deemed unnecessary. Service providers are thereby left to set their own standards. However, with little government oversight, service providers tend to cost-shift by expecting users to be aware of the risks. Terms and conditions are wrapped in legal jargon and buried in lengthy Terms of Service statements that most users do not understand, or bother to read. That service providers create this environment without accepting responsibility for the consequences is cause for concern from a moral standpoint.

I will now provide a broad survey of U.S. privacy policies that might scrutinise ownership and control over personal data, as well as its use and misuse. Throughout, I will apply a Marxist political economy perspective to the development of policies and cases at hand, as Fuchs (2013) usefully did in analysing forms of digital labor. Primary sources include reports and rulemaking activities from regulatory agencies, such as the Federal Trade Commission (FTC) and Federal Communications Commission (FCC); relevant case law in which plaintiffs alleged harm from the missorting of their personal data; and executive actions from Barrack Obama's Presidential administration. Secondary sources used to examine cases of panoptic missorting include the FCC's

consumer complaints database (see https://www.fcc.gov/consumer-help-center-data), as well as popular and trade press reporting. Lastly, I return to Gandy's consideration of missorts in the era of big data to examine the tensions between data based knowledge and cultural wisdom, as well as between political rhetoric and policy reasoning. These tensions pervade a discriminatory and hegemonic U.S. privacy regime.

## The problem of U.S. media privacy policy

Although, the Fourth Amendment to the U.S. Constitution provides for the right of the people to be secure in their person and property from unjust searches and seizures by state authorities, it does not provide such explicit protection against the collection of personal information by private entities. Industry self-regulation tends to be the preferred means of addressing privacy concerns. The low level of state involvement is due to the neoliberal economic policy "emphasis on individualism, First Amendment rights, constraints on government power, and limited regulation of the activities of private entities" (Brown and Blevins, 2002: 569). While privacy is recognised as a legal right in the U.S., it has not been addressed as such in a comprehensive federal statute. Instead, privacy issues belong to a subdivision of federal and state laws that provide limited protection depending upon specific circumstances (see Schwartz, 2009). While there were legislative proposals aimed at more comprehensive consumer data privacy regulation in the 1999 and 2000 Congressional sessions, none came to fruition. A strong industry lobbying effort stalled lawmakers and further rationalised self-regulation to the public (see Brown and Blevins, 2002). It was over ten years before another window of opportunity opened for a full consideration of privacy policy in the United States.

### *The Consumer Privacy Bill of Rights Act of 2015*

Since the 106th Congress, the most notable privacy policy initiative came from the Presidential Administration of Barack Obama in The Consumer Privacy Bill of Rights Act of 2015 (CPBRA, 2015). This White House proposal, released on 27 February 2015 called for a system of industry self-regulation in which businesses would create their own codes for handling consumer information. The FTC was granted oversight to ensure that those codes satisfied certain rights for consumers to: (1) understand how the data will be used; (2) see and correct data held by a company; (3) keep data in the proper context and (4) remove their data (CPBRA, 2015). The 2015 bill was a follow-up to the FTC's (2010) report, "Protecting Consumer Privacy in an Era of Rapid Change" and the Obama Administration's 2012 report, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (2012). None of these efforts received significant support in a Republican controlled Congress and the CPBRA did not advance through the legislative process.

The 2015 CPBRA would have applied to data captured by online businesses, advertisers or third-party aggregators. The proposed Act called for "concise and easily understandable" explanations of how data would be used and, moreover, options for customers to correct and remove information. The latter call would have helped to remedy missorts, especially when economic valuations were being made based upon the data. However, the CPBRA did not specify any industry responsibility for providing information to consumers (in relation to the type of privacy risk). Instead, the CPBRA (2015) only "encourages companies engaged in online advertising to refrain from collecting, using, or disclosing personal data that may be used to make

decisions regarding employment, credit, and insurance eligibility or similar matters that may have significant adverse consequences to consumers" (26). The 'encouragement' proposed in the CPBRA was far short of an actual 'requirement' for accountability and accuracy. The problem here is that innocuous data, when taken out of proper context creates an incomplete, or inaccurate depiction of an individual.

While the CPBRA failed to become law, the FCC was able to pass new privacy rules the following year. At the time of writing, this administrative initiative faces an uncertain future with the election of Donald Trump as U.S. President. There may be changes in administrative appointments to the FCC beginning in 2017.

### *Title II Reclassification and the FCC's new broadband privacy rules, 2016*

The FCC (2016a) introduced a Notice of Proposed Rulemaking in March 2016 to protect the privacy of broadband and telecommunication services customers under Section 222 of the Communications Act (CA). The FCC's (2016a) proposal was made possible by the reclassification of broadband Internet access providers as common carriers under Title II of the CA and Section 706 of the Telecommunications Act of 1996 (TCA). Section 222 of the CA requires that telecommunication companies protect their customers' "proprietary information" gathered from use of service. This entails "the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer" and includes other information "that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship". While this may not be significant in terms of traditional landline telephony usage, it may apply to broadband and mobile Internet Service Providers (ISPs), and could potentially cover information about individuals' web browsing, such as key word searches, sites visited and items purchased. Additionally, the FCC could require broadband and mobile service providers to get users' permission before collecting and sharing their personal data. After Title II reclassification, consumer rights groups petitioned the FCC to develop further requirements for ISPs to disclose their data collection practices, report data breaches and be held accountable when breaches occur (see Consumer Watch, 2016).

The FCC (2016b) formally adopted the new privacy rules for broadband and mobile ISPs, which require a mix of 'opt-in' and 'opt-out' provisions for customers, as well as transparency and data security requirements. For instance, the new rules require that customers must 'opt-in' before their ISPs can use their sensitive data, such as geographic location, communications content, web browsing history, financial information, etc. Only an 'opt-out' provision is required for non-sensitive data, such as email addresses and service-tier information about customers. The requirements for transparency include a provision that ISPs should inform customers how they collect, use and share their personal data. New data security rules encourage ISPs to adhere to industry standard best practices.

Because broadband companies like Comcast and mobile telecommunication providers like AT&T have never been subject to such privacy rules before, there remains a lot of uncertainty about how exactly the new rules will be interpreted and applied by the FCC (and over the kinds of court challenges that may arise from enforcement efforts). Moreover, the FCC's (2016b) rules are a minimal effort, similar to the CPBRA, and do not hold ISPs accountable for the discriminatory and exploitative effects of panoptic missorting. Internet Service Providers cannot refuse service to customers who do not consent to the sharing of their personal data for commercial purposes.

However, the new rules do not prohibit 'pay-for-privacy' plans in which lower cost service plans are offered to customers who consent to the tracking of their online behavior.

### *Panoptic missorts: discrimination, exploitation and lack of accountability*

Although the FCC has made a historic effort through its recent rulemaking to provide greater privacy protection online, the ill effects of panoptic missorting remain, including discrimination, exploitation and lack of accountability. The 'pay for privacy' plans left open by the FCC's (2016b) broadband privacy rules contrasts with the kind of policy petitioned for by the American Civil Liberties Union (ACLU), 18 Million Rising, Black Alliance for Just Immigration and a host of other civil rights organisations. On 16 March 2016, they sent FCC Chairperson Tom Wheeler a letter asking the agency to consider the negative impact that privacy tiers would have on historically disadvantaged communities. The letter (ACLU, 18 Million Rising, Black Alliance for Just Immigration, et al., 2016) warns that the segmenting of customers into service tiers, and the use of predictive analytics can facilitate discriminatory marketing practices. Furthermore, the letter noted that Blacks and Hispanics were more likely than Whites to rely on mobile broadband services and thus, were more vulnerable to the ill effects of data based sorting, and missorting.

Such discriminatory sorting, missorting and predictive analytics can also lead to the exploitation of low-income customers. For instance, Cable One, a cable television and Internet service provider uses predictive analytics (based on low FICO credit rating scores) to define what it calls "hollow value" customers (see Frankel, 2016). In Cable One's view, these customers are more likely to dispute their bill, and not pay regularly and are less likely to purchase higher end services. Therefore, customers sorted into this category (fairly or not) receive less time and attention from customer service representatives. They are not greatly concerned about whether or not the customer in question has actually paid his or her bill on a timely basis; the only thing that matters is that the customer has been sorted into the 'hollow value' file. This is especially concerning, as an FTC report shows that about one in five American consumers have errors on at least one their credit reports (FTC, 2013).

Moreover, correcting missorts of one's personal financial data can be a hellish task, and the institutions that use and share the inaccurate information are not likely to be held accountable for the harm caused to an individual. This was the case in *Nahid Noori v. Bank of America* (2016) when the defendant, Bank of America, erroneously reported to multiple credit rating agencies that the plaintiff, Nahid Noori, was deceased. Although Noori notified Bank of America of the error, she alleged that Bank of America had continued to report her as deceased. This caused her subsequent credit requests to be denied, including one for a home mortgage. However, the court granted Bank of America's motion to dismiss the case, as the plaintiff failed to produce supporting documentation for the loan denials. More notably perhaps, the court found no evidence to support Noori's claims that California's Unfair Competition Law (UCL), the Fair Credit Reporting Act (FCRA) and the Consumer Credit Protection Act (CCPA) had been violated. The court accepted that Bank of America maintained 'reasonable procedures' for credit reporting that were in accord with industry standards. It can be argued that the plaintiff in this case could have taken better care of her own personal data file to ensure the accuracy of crucial information, especially given the consequences or inaccurate data. Nevertheless, in this case, a corporate entity represented a class interest that controlled the ownership and distribution of data, while exploiting a subordinate class of individuals (who that data purports to represent) through favorable state regulatory policies.

One of the key problems with accepted industry standards for data collection and dissemination is that they can "make mistakes with significant consequences" even though they may "appear so flawless that they receive the benefit of the doubt in disputes about accuracy" (Mosco, 2014: 147). Another problem is that it is difficult for plaintiffs to demonstrate the harm incurred from missorts of their personal data. This was the question presented to the U.S. Supreme Court in *Spokeo v. Robins* (2016), after Thomas Robins brought a claim under the FCRA against Spokeo.com, "a people search engine," which offers a listing of individuals' personal information, public records, and social networks in a searchable database. Robins claimed that Spokeo's profile of him contained false information about his financial and marital status – indicating that he was wealthy, employed in a professional field, and married with children. In fact, Robins is unemployed, unmarried and childless; and he asserted that Spokeo's inaccurate profile of his personal data hampered his job search. Prospective employers might conclude from the Spokeo profile that he is overqualified for the positions being applied for and that he would demand a higher salary than he was likely to receive in practice. It might also be assumed that he would be unwilling to relocate (due to the false report of him having a family). The trial court dismissed Robins' claim due to lack of standing, as he could not prove actual harm. The Ninth Circuit Court of Appeals reinstated Robins' claim before Spokeo appealed to the Supreme Court, which remanded the case back to the Ninth Circuit by a 6-2 vote to consider the substantiation of injury caused by the reporting of false information. The Court indicated that "intangible injuries" may be considered, which raises a central question about how the FCRA is currently applied. How does one prove an intangible harm caused by the reporting of false data under the FCRA so that data brokers can be properly held accountable? The difficulty presented here is yet another example of the alienation experienced by the victims of panoptic missorting. State policies reinforce the rights of corporate vendors of data, but provide little to no power to the prosumers of that data. Perhaps, the answer is not in a statute, but in the common law for personal privacy.

Youm and Park (2016) have explained that intrusions of personal privacy in the U.S. not involving "governmental authority" are most often "addressed as a matter of torts and consumer protection" (275). While there are very few statutory privacy protections, there are four primary types of privacy torts that are commonly recognised: disclosure of private facts, intrusion and trespass, appropriation and false light. Although false light is often confused as a libel tort (so much so that many state courts do not recognise false light as a separate tort from libel), it remains in the milieu of privacy torts because it concerns the representation of an individual in a false or highly offensive manner before the public. The primary difference between libel and false light torts is that libel involves defamatory content that significantly injures one's reputation, while there is a lesser standard for false light – an erroneous public portrayal may have caused personal harm without doing reputational damage. In California, where both the *Nahid Noori v. Bank of America* (2016) and the *Spokeo v. Robins* (2016) cases originated, false light privacy torts may also entail untrue implications reasonably drawn from statements (see Digital Media Law Project, 2016). Similarly, panoptic missorts of this variety do not necessarily defame, but rather cause some form of personal harm because of the conclusions drawn from inaccurate or non-contextualised data. However, for the false light privacy principle to work as a recourse for prosumers of missorted data, the appropriate balance between the contextual integrity and corporate speech rights need to be found.

### *Balancing contextual integrity and free expression*

Nissenbaum (2009) has discussed the concept of 'contextual integrity' wherein technology poses significant challenges to people's expectation of privacy. After data is collected in one setting, how it is interpreted may vary when shared with other entities. On this matter, Solove (2008) notes the distinction between information collection and information dissemination. While data collection practices may be sound, the potential for missorting and misrepresentation occurs when the data is disseminated, as changing the context changes the meaning of the data. An important question arises here - does data that casts a false light deserve absolute First Amendment protection?

Tribe (2016) submitted a First Amendment-based argument opposing the FCC privacy rules on behalf of a triumvirate of broadband trade associations, including CTIA–The Wireless Association, the National Cable & Telecommunications Association (NCTA), and U.S. Telecomm. They broadly claimed that privacy rules "would violate the First Amendment" and impose "content-based distinctions" on marketers' speech. In a similar vein, Bambauer (2014) argued that First Amendment protection should apply to data, and thus, data collection should be protected from comprehensive privacy regulation. However, Bambauer (2014) makes one important distinction in her analysis: "data" is "presumed to be accurate" (66). When data turns out to be inaccurate, even through "unintentional error," Baumbauer conceded that it "presents some interesting First Amendment and legal liability questions" (66). While Baumbauer (2014) did not articulate the uncertainties concerning speech rights and responsibilities related to inaccurate data, these are significant issues which are embedded within relations of power.

Because Supreme Court jurisprudence has steadily expanded corporate speech rights, serious questions arise about the balance of power between humans and corporations under the First Amendment (see Blevins, 2014). For instance, in *Sorrell v. IMS Health, Inc*. (2011), the Court struck down a Vermont law that would prohibit pharmacies from selling information about physicians' prescribing habits to pharmaceutical marketers and data miners without the consent of the prescriber. The prohibition was seen as an unconstitutional restriction of corporate speech. In my view, this judgment sets "an alarming precedent that corporate rights to information for commercial purposes is greater than physicians' privacy or patients' interests in affordable medications" (Blevins, 2014: 219). The original Vermont law was intended to protect the rights of physicians and patients. As established in this case and the others presented here, there are clear conflicts between the rights of corporations to sort and missort data under the broad protection of the First Amendment and individual rights to privacy and accurate representation.

Although broadband and mobile ISPs are concerned about the additional cost of conforming to the new rules and the risk of FCC fines, liability for the ill effects of panoptic missorting should not fall exclusively on consumers. Too often service providers shift all moral and legal responsibility upon their customers through Terms of Service that invoke the 'Third Party Doctrine'. This is the idea

> that when information is shared with a third party, the sharer cannot reasonably assume the information will be kept private since the sharer has no control over what the third party might do with that information. Accordingly, any expectation that the information remain private after the sharing with the third party is unreasonable (Armijo, 2014: 411).

These Terms of Service agreements expect users to understand that the service provider is virtually free of any liability for what happens from the use of their personal data by third parties.

*Consent of the missorted?*

Together, the aggrandizement of corporate speech rights, and Terms of Service statements that invoke the third party doctrine, produce a hegemonic environment that appears to manufacture the consent of sorted and missorted subjects. Corporate supremacy over individual privacy rights is maintained by

> coercion [that] is mainly social in nature. Large platforms like Facebook have successfully monopolised the supply of certain services, such as online social networking, and have more than a billion users. This allows them to exercise a soft and almost invisible form of coercion through which users are chained to commercial platforms because all of their friends and important contacts are there and they do not want to lose these contacts. Consequently, they cannot simply leave these platforms. (Fuchs, 2013: 20)

As Fuchs (2013: 20) further explained, individuals are coerced by fear of isolation and social disadvantage if they leave digital media platforms, and social media platforms in particular. Thus, human experiences in digital and social media are shaped by relations of power based on capital even though users do not own the instruments of their own labor. Private companies that commodify that labour, own and control the means of production as well as the products of user generated data. The capitalisation of big data alienates the individuals that generate that data and exploits their labor in creating it (see Fuchs, 2013: 20). Without change, the current policy regime which is premised on industry self-regulation and cultural acceptance of corporate speech rights will continue to thwart user privacy online.

## Conclusion: The hegemony of U.S. digital media privacy policy

This study began with a reexamination of Gandy's (1993) 'panoptic sort' within the contemporary digital environment of big data. While bias along the lines of race and class still occurs, this analysis has shown another disturbing byproduct of current online data gathering and the panoptic machine whose operation it supports - the misrepresentation of individuals through a 'missort' of their personal information. The missort is a mismeasurement and a miscalculation that occurs when data is processed, reprocessed and standardised in terms of meaning. The varying degrees of imprecision that arise reflect a measurement system that works to dichotomise information and fix its cultural meaning. If the panoptic sort (as originally described by Gandy) generates efficiency, the panoptic missort generates inefficiency, and potential harm. Additionally, this analysis has shown that current U.S. privacy law does not provide adequate redress for the victims of discrimination and exploitation as result of panoptic missorting. And, data brokers are not held accountable for the harm caused.

I have endeavored to further critical political-economic theory in this area by questioning the hegemony of ownership and control over personal data, and by calling for a rethink of U.S. privacy policy. Allowing the subjects of panoptic sorting and missorting to at least correct the record when necessary would avoid civil suits - a positive outcome for the public interest and business interests. Without some form of access, control, and redress, the subjects of digital media surveillance will remain misrepresented to prospective employers, health insurers, friends, and associates. Moreover, they may suffer the consequences of economic and social decisions that were made about them based upon missorted information.

Finally, this analysis suggests that future political-economic research should frame resistance to missorts of big data within the concept of false light privacy torts and as part of a general political challenge against the hegemonic discourse of U.S. media policy. Too often, concerns about digital media privacy in the U.S are dismissed under the broad banner of the First Amendment (see Tribe, 2016; and Bambauer, 2014). Free enterprise rhetoric, or platitudes about 'having nothing to hide' influence a U.S. privacy policy which provides little recourse for victims of privacy abuse. Some individuals may 'consent' to all of this data-collection and third-party transfer of their personal data. However, they do not necessarily understand how such data are aggregated and analysed (and the political-economic implications which might follow). Perhaps, most importantly, they have no power to negotiate the terms of service with data brokers and service providers. Leaving digital and social media platforms raises the prospect of losing personal contacts and experiencing subsequent "communicative impoverishment" (Fuchs, 2013: 21). Thus, individuals may only accept or reject the terms and conditions offered. That is a hegemonic form of power (in contradistinction to Lash's suggestion that 'hegemony' as a concept has outlived its usefulness in the big data era). In my view, hegemonic power is manifested in the U.S. policy framework that governs the transfer and panoptic sort of data.

Under these circumstances, false light grievances may be a potential avenue of redress for victims of panoptic missorting. In the meantime, future critical research should continue to illuminate the hegemonic nature of big data ownership and control, as well as emphasising the need for redrawing U.S. media privacy policy. While data brokers are likely to fight to protect their algorithms as trade secrets, consumer privacy advocates should seek further grounds for individuals to access, amend and contextualise the data files of their personal information, especially those generated through their prosumption activities.

## Author Bio

Jeffrey Layne Blevins, Ph.D., is an associate professor and Head of the Department of Journalism at the University of Cincinnati, where he also holds courtesy appointments in the Department of Communication, and the Department of Political Science. His research interests include political economy of media, and media law and policy.

## References

ACLU, 18 Million Rising, Black Alliance for Just Immigration, et al (2006) Letter to

FCC Chairman Tom Wheeler regarding broadband privacy rulemaking. Available at: https://static.newamerica.org/attachments/12815-oti-joins-coalition-urging-fcc-to-consider-civil-rights-principles-for-the-era-of-big-data/20160316%20-%20Broadband%20Privacy%20Letter%20FINAL. dac7b3d835cf41da93f5dfa0f9093dc9.pdf (accessed 15 November 2016).

Armijo E (2014) Communication law, technological change, and the new normal. *Communication Law & Policy* 19(4): 401-415.

Bambauer J (2014) Is data speech? *Stanford Law Review* 66: 57-119.

Beer D (2009) Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society* 11(6): 985-1002.

Blevins JL (2001) Counter-hegemonic media: Can cyberspace resist corporate colonization? In B Ebo (Ed) *Cyberimperialism? Global relations in the new **e**lectronic frontier* (pp. 139-151). Westport, CT: Praeger.

Blevins JL (2014) Political economy of corporate power and free speech in the United States. *Media Watch* 5(2): 209-222.

Brown DH and Blevins JL (2002) The Safe Harbor agreement between the United States and Europe: A missed opportunity to balance the interests of e-commerce and privacy online? *Journal of Broadcasting & Electronic Media* 46(4): 565-585.

CBS News (2014) The data brokers: Selling your personal information. Available at: http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/ (accessed 15 November 2016).

Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934).

Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

Consumer Credit Protection Act of 1968, Pub. L. No. 90-321, 82 Stat. 146 (1968).

Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy (2012) Available at: https://www.whitehouse.gov/sites/default/files/privacy-final.pdf (accessed 15 November 2016).

Consumer Privacy Bill of Rights Act (2015) Available at: https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [https://perma.cc/4AC6-H8YJ] (accessed 15 November 2016).

Consumer Watch (2016) Consumer groups back FCC rulemaking on internet privacy protections. Available at: http://www.consumerwatchdog.org/ newsrelease/consumer-groups-back-fcc-rulemaking-internet-privacy-protections (accessed 15 November 2016).

Couldry N and Powell A (2014) Big data from the bottom up. *Big Data & Society* 1(2): 1-5.

Dick PK (1987) *The minority report.* New York, NY: Pantheon Books.

Digital Media Law Project (2016) Available at: http://www.dmlp.org/legal-guide/california-false-light (accessed 15 November 2016).

Dutta S and Bilbao-Osorio B (2012) The global information technology report 2012: Living in a hyperconnected world. Available at: http://reports.weforum.org/global-information-technology-2012/ (accessed 15 November 2016).

Experian Marketing Services (2014) Mosiac USA: The consumer classification solution for consistent cross-channel marketing. Available at http://www.experian.com/assets/marketing-services/brochures/mosaic-brochure-october-2014.pdf (accessed 15 November 2016).

Fair Credit Reporting Act of 1970, Pub. L. No. 91-507, 84 Stat. 1114 (1970).

Federal Communications Commission (2016a) *Protecting the privacy of customers of broadband and other telecommunications services*, WC Docket 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (*Broadband Privacy Notice of Proposed Rulemaking*). Available at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf (accessed 15 November 2016).

Federal Communications Commission (2016b) FCC adopts broadband privacy rules. WC Docket 16-106, Report and Order 16-148. Available at: https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules (accessed 15 November 2016).

Federal Trade Commission (2010) Protecting consumer privacy in an era of rapid change. Available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf (accessed 15 November 2016).

Federal Trade Commission (2013) In FTC Study, five percent of consumers had errors on their credit reports that could result in less favorable terms for loans. Available at: https://www.ftc.gov/news-events/press-releases/2013/02 /ftc-study-five-percent-consumers-had-errors-their-credit-reports (accessed 15 November 2016).

Frankel, D (2016) Cable One using FICO scores to qualify video customers, Might says. *FierceCable*. Available at: http://www.fiercecable.com/cable/cable-one-using-fico-scores-to-qualify-video-customers-might-says (accessed 15 November 2016).

Fuchs C (2013) Theorising and analyzing digital labour: From global value chains to modes of production. *The Political Economy of Communication* 2(1): 3-27.

Fuchs C and Mosco V (2012) Marx is back! The importance of Marxist theory and research for critical communication studies today. *tripleC: Communication, Capitalism & Critique: Journal for a Global Sustainable Information Society* 10(2): 127-140.

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

Gramsci A (1996) *Prison Notebooks.* Columbia University Press. IBM (2015) Bringing big data to the enterprise. Available at: http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html (accessed 16 November 2016).

Lash S (2007) Power after hegemony: Cultural studies in mutation? *Theory, Culture & Society* 24(3): 55-78.

Meehan E, Mosco V and Wasko, J (1993) Rethinking political economy: Change and continuity. *Journal of Communication* 43(4): 105-116.

Mosco V (2009) *The political economy of communication*, 2nd ed. Thousand Oaks, CA: Sage.

Mosco V (2014) *To the cloud: Big data in a turbulent world*. Boulder, CO: Paradigm Publishers.

*Nahid Noori v. Bank of America*, Case No. 15-01467, C.D. Calif.; 2016 U.S. Dist. LEXIS 76141 (2016).

National Science Foundation (2015) White paper for privacy in an era of big data workshop, Temple University, Philadelphia, PA. Available at: http://www.fox.temple.edu/cms_research/privacy-in-the-era-of-big-data/privacy-in-an-era-of-big-data-2/ (accessed 16 November 2016).

Nissenbaum H (2009) *Privacy in context: Technology, privacy, and the integrity of social life.* Stanford, CA: Stanford Law Books.

Schwartz PM (2009) Preemption and privacy. *Yale Law Journal* 118: 902-947.

Singer N (2015) Sharing data, but not happily. *The New York Times*. Available at: http://www.nytimes.com/2015/06/05/technology/consumers-conflicted-over-data-mining-policies-report-finds.html?_r=0 (accessed 16 November 2016).

Solove DJ (2008) *Understanding privacy*. Cambridge, MA: Harvard University Press.

*Spokeo, Inc. v. Robins*, 578 U.S. (2016) Available at: https://www.supremecourt.gov/opinions/15pdf/13-1339_f2q3.pdf (accessed 16 November 2016).

*Sorrell v. IMS Health, Inc.*, 131 S.Ct. 2653 (2011) Available at: https://www.supremecourt.gov/opinions/10pdf/10-779.pdf (accessed 21 November 2016).

Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56. (1996).

Tribe L (2016) *The Federal Communication Commission's proposed broadband privacy rules would violate the First Amendment*. White paper commissioned by the National Cable & Telecommunications Association, United States Telecomm Association, and Cellular Telephones Industry Association and submitted to the Federal Communications Commission.

Turow J (2012) *The daily you: How the new advertising industry is defining your identity and your worth*. Yale University Press.

Turow J, Hennessey M & Draper, N (2015) The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. A report from the Annenberg School for Communication, University of Pennsylvania. Available at: https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf (accessed 16 November 2016).

U.S. Senate, Committee on Commerce, Science and Transportation (2013) A review of the data broker industry: Collection, use and sale of consumer data for marketing purposes. Available at: https://www.commerce.senate.gov/ public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf (accessed 16 November 2016).

Youm KH and Park, A (2016) The 'right to be forgotten' in European Union law: Data protection balanced with free speech? *Journalism & Mass Communication Quarterly* 93(2): 273-295).