2017

The limits of transparency: Data brokers and commodification

Matthew Crain
CUNY Queens College

Article

new media & society
1–17

DOI: 10.1177/1461444816657096
nms.sagepub.com
SAGE

The limits of transparency: Data brokers and commodification

Matthew Crain
Queens College, City University of New York, USA

Abstract
In the United States the prevailing public policy approach to mitigating the harms of internet surveillance is grounded in the liberal democratic value of transparency. While a laudable goal, transparency runs up against insurmountable structural constraints within the political economy of commercial surveillance. A case study of the data broker industry reveals the limits of transparency and shows that commodification of personal information is at the root of the power imbalances that transparency-based strategies of consumer empowerment seek to rectify. Despite significant challenges, privacy policy must be more centrally informed by a critical political economy of commercial surveillance.

Keywords
Commodification, data brokers, privacy, public policy, surveillance, transparency

Shortly after Edward Snowden revealed the massive scale and scope of the National Security Administration's communications surveillance programs, Federal Trade Commissioner Julie Brill took to the editorial pages of the *Washington Post* to raise another alarm. Brill sought to draw attention to a group of transnational corporations called data brokers that, like the National Security Agency, make it their business to know everyone's business. The Commissioner argued that these companies had operated in the shadows of public awareness and regulatory oversight for too long. Data brokers such as Acxiom, Experian, and ChoicePoint were secretly gathering information about millions of people and distributing it to clients for a wide range of uses. The time had

Corresponding author:
Matthew Crain, Media Studies, Queens College, City University of New York, 65-30 Kissena Blvd, Queens, NY 11367-1597, USA.
Email: mcrain@qc.cuny.edu

come to demand "transparency from the commercial data brokers that know much more about us than we do about them" (Brill, 2013).

The call for transparency is a common refrain in debates about the overreach of private and state surveillance alike. Brandeis' (1913) famous phrase, "sunlight is the best disinfectant," highlights the role of transparency as a pillar of liberal democratic values. In many ways, this is an easy position to support: meaningful understanding of circumstances is a prerequisite for self-determination. In the case of data brokers, transparency proponents argue that consumers need access to information about monitoring practices in order to make rational decisions about their personal data. This can be accomplished if companies engaging in data collection simply give consumers a seat at the table. In Commissioner Brill's (2013) words, "There is no reason that data brokers and firms that use consumer data cannot coexist with a system that empowers consumers to make real choices about how our private information is used."

This essay makes the opposite case. Transparency, while a laudable goal in many respects, runs up against insurmountable structural limitations within the political economy of the data broker industry. While the intentions of transparency advocates are commendable, this policy approach is subsumed by a discourse of consumer empowerment that has been rendered meaningless in the contemporary environment of pervasive commercial surveillance. Data brokers will not—and indeed cannot—cede control over marketing data to consumers themselves without a significant reorientation of their industry. Utilizing historical methods, including close reading of business documents, official regulatory reports, and press coverage, this essay employs political economic analysis to diagnose the limits of transparency and interject a theory of commodification into policy debates. I argue that commodification of personal information lies at the root of the power imbalances that transparency-based strategies of consumer empowerment seek to rectify. While there are significant challenges for designing and implementing public policies aimed at commodification, regulatory approaches that sidestep the issue will remain largely ineffectual. Although these matters are of international concern and the European Union is an especially relevant comparative case, I limit my analysis to the United States. With that delineation, however, the main thrust of a commodification-based critique of transparency is potentially generalizable beyond the US context.

I begin by outlining the data broker industry and its fundamental characteristic of privacy asymmetry. I then survey recent regulatory and legislative efforts to introduce transparency into data broker operations in the United States. Examining one major data broker's response to this political pressure illustrates two limits of transparency. On one hand, the industry's structure and operations impede meaningful transparency in significant ways. On the other, data brokers appropriate transparency values in public relations efforts to deflect the threat of government regulation. This follows a well-worn pattern in Internet history whereby commercial monitoring is legitimized under a rubric of consumer choice. As a consequence, transparency initiatives have created the illusion of reform while leaving basic power imbalances intact. In the final sections I argue that data brokers are better understood via the lens of commodification, rather than consumer empowerment, and that public policy must be more centrally informed by a critical political economy of commercial surveillance.

Data brokers and privacy asymmetry

Data broker is an imprecise term. It generally refers to companies that specialize in the collection and exchange of personal information and is usually associated with large-scale, "big data" operations. Major data brokers, also called "information resellers," such as Acxiom and Experian have roots in established business sectors like direct marketing and credit reporting. Others like Rapleaf and Datalogix were formed to capitalize on the possibilities for data collection and analysis engendered by networked communications and computing. Data brokers' sources, methods, and clients are diverse, but as a group they operate at the heart of the expanding industry of commercial surveillance. The global data broker industry is estimated to comprise thousands of companies of various sizes generating some US$200 billion in annual revenue (Mott, 2014).

The business of data brokers can be classified into two basic processes of data acquisition and data monetization. Data brokers collect a broad array of consumer information on a massive scale. As of 2014, Acxiom alone claims to retain over 3000 pieces of information for nearly every adult consumer in the United States and offers "multi-sourced insight into approximately 700 million consumers worldwide" (Acxiom Corporation, 2014: 8). Without detailing the universe of information data brokers collect, we can generalize by saying that virtually nothing is out of bounds. Demographic, economic, behavioral, health, religion, sexuality, and life event–based information are all routinely aggregated.

While data brokers obtain information directly from consumers to varying degrees, firsthand collection is overshadowed by two other forms of acquisition: (1) buying consumer data from private companies and government agencies and (2) trawling public information generated by the state such as property records, voter and motor vehicle registrations, court records, and census data. Many companies and government entities sell their customer information as an additional revenue stream or exchange data as part of service agreements. Walt Disney, for example, sells the age and gender of its customers' children to third party marketing partners (Beckett, 2014). The US Post Office has long sold lists of recent movers to companies looking to market to relocating households. Regarding public records, data brokers employ staff to gather this information on a regular basis through online databases, records requests, or simply sending researchers to county clerks' offices. On the monetization side, data brokers use consumer data like raw materials to create various informational goods and services. The majority of the industry is not consumer-facing, serving instead institutional clients large and small, from companies to non-profits to government agencies (Federal Trade Commission [FTC], 2014: 23). Data brokers offer products and services integral to a range of business activities including marketing, risk mitigation, and identity verification, as well as federal and state law enforcement and counter-terrorism.

Many Americans are aware of commercial monitoring in a general sense and express desire for increased control over marketing data practices (Turow et al., 2015). At the same time, people generally have only a vague understanding of the extent of commercial monitoring and largely misconstrue actual practices of data collection and the public policies that govern them (Whittington and Hoofnagle, 2012). As a former privacy

lawyer told *60 Minutes*, "It's not about what we know we're sharing, it's about what we don't know is being collected and sold about us" (Messick and Gavrilovic, 2014).

These surveillance practices are characterized by what Andrejevic (2007: 7) calls an "asymmetrical loss of privacy." The basic observation is that people are opened up to increasingly extensive forms of monitoring, while the institutions doing the monitoring and the information they collect remain hidden from view. Privacy asymmetry as a descriptive category is especially salient for the data broker industry, which has long operated without public awareness or direct regulatory oversight. The privacy of those under watch is undermined, while the watchers themselves operate with substantial freedom from scrutiny. Individuals, to the extent they are aware of data brokers at all, can only engage with them under severe informational deficits. Privacy asymmetry also characterizes the relationship among data brokers and regulatory agencies, which have struggled in recent years to compel data brokers to reveal operational details. As I will demonstrate, these informational tensions express a fundamental division that stems from data brokers' commodification of personal information.

Regulatory scrutiny and industry response

While data brokers have historically faced limited governmental oversight, the sector has recently attracted the attention of regulators, elected officials, news organizations, and civil liberties groups. Generally speaking, these groups have embraced transparency as a seemingly straightforward response to privacy asymmetry. As the primary government agency involved in consumer privacy protection, the FTC has been at the forefront of efforts to investigate data brokers. Spurred on by a series of data security breaches in the 2000s, the FTC included data brokers within the scope of broader efforts to address growing concerns over online privacy (FTC, 2012: 69). In 2012, the Commission took a major step in recommending that Congress consider targeted legislation "to address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information" (FTC, 2012: v). In a subsequent report, the FTC identified "a fundamental lack of transparency about data broker industry practices" (FTC, 2014: vii). The White House (2012) reinforced this message by asking Congress to enact a "Consumer Privacy Bill of Rights." President Obama's administration drew specific attention to data brokers' aggregation of "personal data from multiple sources, often without interacting with consumers at all" (White House, 2012: 13).

Legislators in both houses of Congress opened separate investigations into the data broker industry and called company executives to Capitol Hill for hearings (Singer, 2012; US Government Accountability Office, 2013). Senate Commerce Committee Chairman Jay Rockefeller unfavorably compared data broker monitoring to the secret surveillance programs of the National Security Administration (Tummarello, 2013). Between 2010 and 2015, lawmakers introduced (although did not pass) dozens of bills addressing data privacy and security issues including the Consumer Privacy Protection Act (2011, 2015), Commercial Privacy Bill of Rights Act (2011, 2014), and Data Broker Accountability and Transparency Act (2014), all designed to inject transparency into commercial monitoring.

Industry-specific legislative proposals are not extraordinary as there is no comprehensive federal law governing commercial collection of personal information (Nehf, 2012: 61). Instead, privacy protections regarding certain types of data are covered by disparate statutes (e.g. health information, financial information, telemarketing). As Bennett (1997: 13) argues, the general approach to privacy policy in the United States is "reactive rather than anticipatory, incremental rather than comprehensive, and fragmented rather than coherent." As such, data brokers' marketing activities largely fall outside the scope of existing laws like the Fair Credit Reporting Act, which, among other provisions, requires consumer reporting agencies to provide individuals with access to credit reports.

Despite variation regarding implementation and scope, a fundamental assumption shared among all of these policy efforts is that transparency—the mitigation of privacy asymmetry—is key to consumer empowerment over commercial data collection. The notion that transparency will empower consumers to make advantageous choices regarding their interactions with data brokers lacks immediate credibility simply because data brokers are not consumer-facing companies. The industry has historically operated under the radar of consumer awareness. Nevertheless, transparency has been championed within a broader "Fair Information Practices" framework that positions disclosure as the necessary precursor to individual choice and consent. This logic is prominent at the FTC and frames the title of its 2014 report, "Data brokers: A call for transparency and accountability." It is also evidenced in the comments of then Representative (now Senator) Edward Markey, who pledged to "push for whatever steps are necessary to make sure Americans know how this industry operates and are granted control over their own information" (Calvan, 2012). I offer a substantive critique of this policy approach in the final sections of this essay. For now, the point to emphasize is that "notice and choice" has been the dominant regulatory framework applied to the data broker industry, and indeed much of US privacy policy since the 1970s (Simon, 2000: 132–153).

Responding to this surge of political activity, a number of data brokers have taken steps to become more transparent. In 2013 Acxiom made headlines by unveiling a consumer information portal called About The Data. Acxiom billed the site as a resource for consumers seeking answers to "questions about the data that fuels marketing," and it was received by some observers as a welcome opportunity to peek under the hood of one of the nation's largest data brokers. *CNN Money* described the portal as "a win for privacy advocates who have long called for increased transparency" (Hicken, 2013).

About The Data enables individuals to review some of the information Acxiom has collected about them and the data on display are substantial. The site reveals information across six categories: demographic, residential, vehicle, economic, purchase history, and interests. Within these groups are specific data points regarding age, gender, marital status, occupation, income, credit, home ownership, property type, and online and offline purchasing records. The experience of seeing one's personal information displayed in such a fashion brings the scope of data broker surveillance into sharp relief. Privacy asymmetry is counteracted to the extent that people are enabled to review elements of what are clearly extensive marketing profiles. Furthermore, portal users are given the opportunity to edit and add information and even opt out of certain marketing programs (although the process is convoluted). While Acxiom has not disclosed comprehensive

traffic data, CEO Scott Howe unofficially reported that the site received 500,000 visitors in the first month of release (Watson, 2014).

Two limits of transparency

A global market leader abruptly reversing its long-standing policy of non-disclosure is a significant development that bears scrutiny in the context of ongoing debates about privacy regulation. Acxiom's creation of a consumer data portal is instructive for a broader critique of transparency-based privacy policy. Specifically, About The Data illustrates two significant limitations embedded in efforts to make data brokers more accountable via transparency. The first involves structural impediments. Comprehensive transparency is effectively impossible to implement because privacy asymmetry is a cornerstone of the data broker business model. The second limit is regulatory deflection. Transparency initiatives have historically been deployed to shore up regimes of industry self-regulation, which have repeatedly failed to protect consumer privacy (Hoofnagle, 2006). Following this pattern, Acxiom's portal exemplifies the political expediency of transparency for companies looking to continue or expand their surveillance practices unimpeded by consumer protection regulations.

Drawing upon scholarship from legal studies and political economy of communications, this section develops the Acxiom case study to demonstrate these limits. The most obvious critique of About The Data is simply that it discloses only a small subset of the company's vast stores of consumer information. While Acxiom claims to make 3000 data elements per person available to clients, the site shows consumers a much smaller number, ranging from 50 to 125 attributes (Bryan, 2013). Equally important is Acxiom's framing of its operations: what it says and does not say about *how* the data are obtained and monetized. Although specific data points are disclosed, the portal offers little detail about the sources or destinations of this information. Instead, users are directed to a "Learn" section that vaguely describes how marketing information is gathered from an array of largely un-named sources. The site notes that personal data help to make commercial messaging more relevant, preventing, for example, "advertisers from bombarding you with ads for bicycles if you are a Ferrari aficionado." This type of sanitized language obscures substantive understanding, much in the way that online privacy policies often bury readers in legal jargon (Turow, 2011: 176–181). Detailed information about how data are acquired and monetized lies beyond the bounds of Acxiom's implementation of transparency and the balance of the portal's functionality falls into the realm of public relations.

These inadequacies would seemingly be easy to overcome through more robust disclosure measures. Setting aside for the moment the difficulties human beings face when processing large and complex data sets (Solove, 2013), could data brokers achieve meaningful transparency by releasing comprehensive information about their practices? The answer is no because the structure and operations of the industry are incompatible with a transparency framework of full disclosure. Once information has been swept into the data broker marketplace, it becomes challenging and in many cases impossible to trace any given datum to its original source for any combination of the following reasons: (1) data brokers maintain that information sources and analytic processes are trade secrets,

(2) information buyers and sellers are divorced from information collection by degrees of separation via complex markets, and (3) a significant portion of data brokers' information is computationally generated and therefore has no "real" empirical source.

Citing competitive reasons, data brokers have routinely refused to release details of their business practices to outside entities (US Senate Committee on Commerce, Science, and Transportation, 2013: iii). A powerful "discourse of economic secrecy" (Cohen, 2010: 886) helps to sustain an environment where even Congress has largely failed to compel data brokers to identify information sources and clients. As one executive testified at a Senate hearing, "I can't tell you who our clients are. That's a proprietary list of ours. That's like our secret ingredient" (Tummarello, 2013). Even if data brokers were more forthcoming, information sources are not easily traceable because specific data points are packaged and repackaged, sold and resold in multi-layered markets. One FTC (2014) examination found that nine major data brokers purchased substantial quantities of data from *other data brokers*, who themselves obtained data from various sources, and on and on. The complexities of consumer data marketplaces are intensified as technologies, analytical processes, and business relationships undergo continued development.

While data brokers gather and analyze massive amounts of data, they do not have total information awareness. Confronting information gaps about current and potential customers has always been a fundamental challenge for marketers. Data brokers have responded by developing expertise in inference and prediction, using existing information to model data that are inaccessible or do not exist. Here, a distinction can be drawn between "core data" obtained through various means of surveillance and "derived data" stemming from its algorithmic interpretation. For instance, Acxiom employs modeling to derive data in cases where specific information is missing. Categories of race or ethnicity might be extrapolated from ZIP code and name, or political affiliation might be inferred from home ownership and education. Because they are composites, derived data of this nature disrupt the logic behind calls for disclosing the sources of marketing profile information in order to promote transparency.

In each of these areas the structure and operations of the data broker industry impede transparency initiatives based upon simple forms of information disclosure. Privacy asymmetry is a defining feature of data brokerage. Nevertheless, policy initiatives have largely focused on "requiring data brokers to provide consumers with access to their data … at a reasonable level of detail" (FTC, 2014: 51). Certain recent proposals seek to expand the scope of transparency beyond disclosure toward strategies that approximate what Nissenbaum (2010) calls "contextual integrity." This approach argues that consumers must be given a set of reasonable expectations about how data are used once they have been collected. Whenever possible, these expectations, or "informational norms," should be drawn from analogue social spheres. For example, a coherent set of privacy rules should apply to personal banking across transactional settings such that consumers could expect consistent data policies whether banking online, at the ATM, or the teller window. Pushing against the dichotomy of online and offline, this approach anchors policy to the context of action (e.g. banking, health care) and relieves consumers of the impossible burden of interpreting the output of full disclosure for every instance of data collection and deployment. Along these lines, the Obama administration's proposed

Consumer Privacy Bill of Rights seeks to implement degrees of contextual integrity by limiting the use of consumer data to expressly stated or otherwise "reasonable" purposes (White House, 2012).

Like polices of full disclosure, contextual integrity in this formulation is still about transparency, only at a higher level of abstraction. A constellation of appropriate uses must be made transparent, rather than an absolute account of the operational details. But here again, the data broker industry is confounding because the core of its business model is about *repackaging disparately sourced information to serve purposes other than those for which it was originally obtained*. Data brokers offer myriad products to inform a wide range of decision-making processes, including using analytics to sort people into categories based on predictions of future behavior, for example, to generate sales leads or to make determinations about risk, particularly in the realm of finance. A growing industry sub-sector applies "big data" to underwriting, using a wide spectrum of information from web surfing habits to social network connections to determine credit-worthiness (Morozov, 2013). As one company's slogan put it, "All data is credit data" (Koran, 2015). These and myriad other applications are possible precisely because data obtained in given settings are sold, adapted, and resold to serve "downstream" purposes in new contexts.

While transparency efforts such as About The Data fail to counteract commercial surveillance in meaningful ways, they nevertheless serve important political functions for data brokers themselves, namely, deflecting potential government regulation. This is the second limit of transparency. As internet business models have pivoted around consumer surveillance, maintaining a public policy regime based on industry self-regulation has become a priority for data brokers and the marketing complex at large (Hoofnagle, 2006). US companies have a long history of working together via trade groups and other means to implement self-regulation in order to stave off government oversight. Political economists such as Stole (2006) and Niesen (2012) have shown how the advertising industry, an analogue of data brokers, has been particularly effective in shaping public policy to favor self-regulation, quelling consumer movements that sought government protection against commercial abuse. In this context, what has been framed by Acxiom as a proactive move is clearly a defensive measure: a regulatory deflection dressed up in the trappings of transparency.

Although *The New York Times* described the About The Data portal as "novel" (Singer, 2013), it fits within a well-worn public relations strategy in the business of consumer data collection. In the late 1990s, the first generation of online data brokers used this tactic in contests with regulators and privacy advocates to determine what rules would govern Internet data collection and use, broadly conceived. Although not as sophisticated as contemporary practices, online consumer data collection was nevertheless rampant and largely outside of regulatory purview. Flush with dotcom era finance capital, companies like DoubleClick (now part of Google) and Engage (now part of Microsoft) developed massive consumer profiling and ad targeting capacities, which attracted the attention of privacy advocates who marshaled policy-makers into action (Crain, 2014).

Data brokers, online advertising companies, web publishers, and marketers formed trade groups to fend off regulatory threats and maintain the status quo of advertising industry self-regulation. Their weapon of choice was public relations. When the FTC

found that 85% of major websites collected consumer information while just 14% disclosed such practices, the Direct Marketing Association led a campaign to encourage companies to post privacy policies (FTC, 1998: ii). When most policies proved to be incomprehensible, companies created templates for general use. Even then (and still today), rather than providing genuine transparency, privacy policies "let users know as little as possible about data collection activities, in as polite but complex a fashion as possible so that they wouldn't understand what was going on but could feel good about them" (Turow, 2011: 83). The adoption of privacy policies forestalled action by the FTC, which was persuaded to give the industry more time to develop effective measures of self-regulation.

The conflict escalated as data brokers moved forward with efforts to merge online information with personally identifiable offline data. While a common practice today, the systematic combination of offline and online data was novel at the time and was widely perceived as a violation of privacy norms. With increasing public concern, Congress considered adopting "opt-in" legislation mandating that companies obtain prior consent from web users regarding data collection. Citing a renewed commitment to transparency, companies developed privacy portals like DoubleClick's Privacychoices.org, which provided information about data practices and offered consumers a mechanism to "opt out" of data collection. Although extremely limited in scope and implementation, the opt-out option became generalized enough among online advertising operations to weaken the case for opt-in provisions. Industry self-regulation was established as the default system of governance for online data collection on the basis of a veneer of transparency and consumer choice.

This strategy remains important for Internet companies of all kinds. In 2009, Google created its "Dashboard" privacy control center in the midst of renewed FTC investigations and Congressional privacy hearings. Acxiom's consumer portal is the latest installment in this historical trend and must be understood as a maneuver to manage the risks posed by regulation. About The Data seeks to assuage privacy concerns as part of a larger effort to "evangelize" a "new Acxiom story" (Acxiom Corporation, 2014). It is important to note that the company's transparency efforts have dovetailed with an aggressive growth strategy. According to annual reports to shareholders (Acxiom Corporation, 2012, 2014), Acxiom increased the number of individuals in its global marketing information databases by 40% (from 500 million to 700 million) from 2012 to 2014 and grew the number of data points gathered on US consumers sixfold (from 500 to 3000). Perhaps most importantly, the About The Data site coincided with the release of Acxiom's new Audience Operating System (AOS), a cloud-based platform enabling "marketers to connect all types of traditionally disconnected data and—for the first time—to create a truly singular view of the consumer" (Acxiom Corporation, 2013).

There is a certain degree of instrumental merit to data brokers' efforts to lift the curtain. Acxiom's portal presents a jarring snapshot of the magnitude of commercial surveillance. But the bigger picture is that because the United States has an extremely limited political baseline for consumer data protection, something like AboutTheData is considered "novel" or progressive while deflecting the question of whether transparency is an appropriate policy approach in the first place.

Commodification of personal information

Transparency is deployed as a means to empower consumers to transact with data brokers as equals within information marketplaces. While the FTC (2014) and legal scholars (Nehf, 2012; Pasquale, 2015; Solove, 2013) have recognized the limits of transparency to varying degrees, the policy response has largely been to iterate within the consumer empowerment model, emphasizing self-determination and market fairness. The data broker case study suggests a need for alternative understandings of the policy problems associated with commercial surveillance. The issue is not that transparency has not yet been properly configured; it is that the consumer empowerment frame misunderstands key dynamics of commercial surveillance and therefore offers flawed policy solutions.

Coming from outside the dominant legal paradigm, political economy of communication advances an alternative understanding of commercial surveillance that places commodification at the center of analysis and charts a path for policy to transcend the limits of transparency. This perspective situates data brokers within broader capitalist imperatives and frames the outcomes of commercial surveillance as a structural issue, rather than a problem of transactional fairness. Political economy has developed a multipronged theory of commodification that addresses media content, audiences, and labor (Mosco, 1996). Most relevant here is the concept of audience commodification initially articulated by Smythe (1977) at the height of the US television broadcast era. Smythe argued that the principle product of mass media was not content or ideology, but rather the audience commodity. The core proposition was that advertising-supported media industries produce aggregates of human attention in various forms to be sold to marketers and other entities seeking to influence audience behavior. Reinvigorated by the rise of the Internet and mass media's ongoing adaptation, a burgeoning literature engages audience commodification in the digital age (see McGuigan and Manzerolle, 2014).

The tradition I draw upon here looks to Marx's elaboration of commodification not as a roadmap but as a heuristic for understanding data brokers' acquisition and monetization of personal information and how these processes relate to capitalism's historical development and systematic drives. Building on the work of Schiller (2007) and Mosco (1996, 2009), I focus on commodification as a fundamental process of capitalism that enlarges the social terrain of capital accumulation and reproduces a specific class relation between capital and labor. Far from a strictly top-down activity, commodification is understood as a dynamic and contested process that incorporates the actions of individuals, commercial entities such as data brokers, and state actors like the FTC. However, as will be emphasized below, a key insight of commodification theory is that individuals are compelled to act "within a social field whose terms of engagement are primarily set by capital" (Mosco, 2009: 138).

The acquisition and monetization strategies of data brokers outlined above reproduce and extend the processes of audience commodification identified by Smythe. "Nonrival" inputs are not used up in data broker commodification practices, while the marginal cost of reproducing digital information is essentially zero. These formal characteristics, which led Gandy (2011: 436) to describe information as a particularly "troublesome commodity," have the effect of greasing the wheels of the data broker business model. The more any given data point can be repurposed, the more opportunities are

created for monetization. For example, utilizing a consumer profile to target an online advertisement creates feedback—Did the user click on the ad? Did they make a purchase?—that can then be commodified again and reconstituted as yet another input. This "recursive" (Jordan, 2015) or "cybernetic" (Mosco, 1996: 150) process presents cascading opportunities for monetization that intensify as data brokers form new partnerships.

Recall that data brokers obtain much of their information second hand. Many data broker clients engage in information collection practices of their own, functioning as both buyers and sellers across various markets. Data brokers represent a central node in this matrix of surveillance because they engage in a kind of information arbitrage, buying, repackaging, and selling consumer data across contexts. More than just information collectors and suppliers, data brokers enable information exchange among organizations and create markets for consumer data (via what some economists call "platformization"), which further incentivizes surveillance among many types of entities. In this way, data brokers exemplify what Mosco (1996: 153) terms "extensive commodification," the enlargement of the social terrain of capital accumulation. Acxiom, whose aggressive expansion is noted above, routinely seeks out untapped data sources in order to, in the company's words, "reach everyone who needs to be reached" (Acxiom Corporation, 2016). By facilitating information commodification and exchange among various partners, data brokers connect a multitude of surveillance practices in a "spiral of expanding exchange value … that draws all organizations into the orbit of the information business" (Mosco, 2009: 143). Simply put, commodification of personal information has become one of the Internet's foremost business models.

This historical arc is elucidated by Schiller (1999, 2007, 2014), who connects information commodification to a structural understanding of capitalist imperatives and the increasingly outsized role of information and communication technology in capital's accumulation and crisis mitigation strategies. Capitalism has long been "sustained by ceaseless enlargement of markets for commodities and this trend continues today in information" (Schiller, 2007: 23). Since the latest period of general economic stagnation that began in the 1970s, capitalists have been forced to seek out new markets, incorporating information and communication technologies into the heart of these efforts. This has taken a range of forms including movements to expand transnational consumption, extend intellectual property regimes, and ramp up the technologies and practices of commercial surveillance.

These developments have been characterized as responses to the recurrent problem of overproduction, which is manifested in part by the relentless need to create and maintain consumer demand for the torrent of products and services produced by a capitalist economy dependent upon perpetual growth (Harvey, 1982, 2010). Framing the issue in this way historicizes the commodification of personal information as stemming from the "pan-corporate need to harness consumption to production" (Schiller, 1999: 124). Increasingly, engaging in consumer surveillance is simply the price of doing business for all commercial enterprises. Schiller's approach recalls one of the perhaps less-remembered elements of Smythe's (1981: 25) original effort, which sought to address audience commodification "from the standpoint of its historical-materialist role in making monopoly capitalism function through demand management."

All of this points to data brokers' position within a "surveillance industrial complex" (Ball and Snider, 2013; see also Zuboff, 2015) in which a range of private and public institutions conduct expansive monitoring across communications networks. While managing to avoid revealing specifics, Acxiom was finally compelled by Senate investigators to disclose that its customers in 2013 included

> 47 Fortune 100 clients; 12 of the top 15 credit card issuers; seven of the top 10 retail banks; eight of the top 10 telecom/media companies; seven of the top 10 retailers; 11 of the top 14 automotive manufacturers; six of the top 10 brokerage firms; three of the top 10 pharmaceutical manufacturers; five of the top 10 life/health insurance providers; nine of the top 10 property and casualty insurers; eight of the top 10 lodging companies; two of the top three gaming companies; three of the top five domestic airlines; and six of the top 10 U.S. hotels. (US Senate Committee on Commerce, Science, and Transportation, 2013: 29)

Beyond the private sector, data brokers partner with the Social Security Administration and Departments of Justice, Homeland Security, and State (US Government Accountability Office, 2006).

Ongoing scholarship in political economy explores the ramifications of extensive commodification of personal information. Longstanding debates regarding whether and how media engagement constitutes a form of labor have been extended to digital platforms (Cohen, 2008; Freedman, 2012; Fuchs, 2010) and often highlight the exploitative elements (via capital's extraction of surplus value) and ideological functions of consumption work. These issues have been addressed at length elsewhere (McGuigan and Manzerolle, 2014). For now it is sufficient to consider how commodification of personal information relates functionally to self-determination because self-determination is at the heart of transparency. Commodification is central to a Marxian critique of capitalism in which the basic premise of the labor/capital relation is that workers are compelled to turn their labor power into commodities to be sold to capitalist owners of the means of production. However, this class relation is not only about control over the means of production; it is also about control over the labor commodification process itself. It is about a division between those who set the terms that structure an engagement and those who submit to those terms.

This fundamental power imbalance is mirrored in the dynamics of commodification within pervasive commercial surveillance. An infrastructure of impenetrable monitoring, replete with flaws, miscalculations, and multiple points of resistance, nevertheless structures the terms of everyday engagement with a broadening matrix of activities. Data brokers and other surveillance entities unilaterally control the conditions under which personal information is commodified. Andrejevic (2007) marks the parallels between this "digital enclosure movement" and the historical privatization of public land that enabled a newly propertied class to dictate the terms of access for everyone else. For the modern class of data subjects, submission to monitoring is simply a condition of participation in digital life. Transparently disclosed or otherwise, surveillance itself is not up for negotiation. Ultimately, the self-determination that transparency efforts seek to engender is circumscribed by commodification.

Critics of this position might argue that the class analogy is flawed because individuals are not compelled to use social media, credit cards, online shopping, email, or other terminals of consumer surveillance. However, avoiding commodification of personal information is increasingly unfeasible (Angwin, 2014), precisely because of the system-wide demand management processes outlined above. The choice between submitting to surveillance or "living under a rock" is no choice at all. Unsurprisingly, consumers are increasingly aware of this state of affairs, yet feel powerless to intervene. A recent study by Turow et al. (2015) finds that consumers by and large do not understand commercial data collection within the rubric of fair market transactions. Instead, most people submit to monitoring under a mindset of resignation, believing it "futile to [attempt to] manage what companies can learn about them" (Turow et al., 2015: 3).

Conclusion: confronting commodification

The consumer empowerment policy model sidesteps commodification and neglects its basic insight: people are the products, not the consumers, of the data broker industry and commercial surveillance at large. Consumer empowerment looks to transparency to correct an imbalanced interaction between more or less equal parties. Commodification suggests that unfairness between parties is not a glitch in the system—it is the system. Data brokers' commodification of personal information is deeply entrenched in historical processes of capitalist expansion and will continue to become more widespread and invasive if left unchecked. The result is a fundamentally inequitable social relation, something that transparency alone cannot remedy.

Clearly, this type of diagnosis presents significant policy challenges. Consumer empowerment is rooted in a dominant policy discourse of "corporate liberalism" (Streeter, 1996) in which the government's perceived role is to facilitate the service of individual liberties by private business. When public and market interests diverge, as in cases of online privacy, the government must work to harmonize, but always within a framework where individual needs can be fulfilled by a technologically sophisticated private sector. Capitalist states have long been invested in promoting forms of "marketplace citizenship" (Maxwell, 1999) and the FTC's particular approach to privacy stems from its historical mandate to build consumer trust in online commerce (Bamberger and Mulligan, 2011) and the larger "interpretive community" (Streeter, 1996) of corporate liberalism.

Policies aimed at commodification would challenge these assumptions, face major barriers to implementation, and run head-on into the long-standing antagonism between reform and radical structural change (Luxemburg, 1973; Wright, 2015). This is of course an enduring problem for critical analysis and activism that I do not claim to solve here. As noted above, reformist policies that have intervened into online commercial surveillance have often served to legitimize the regime of commodification of personal information. At the same time, bringing radical change to a deeply entrenched system is, to put it mildly, a "daunting task" (Wright, 2015).

Rather than pointing to a specific set of proposals, this analysis suggests that in order to transcend the limits of transparency, public policy must look beyond consumer empowerment to consider how alternative communications infrastructures might counter commodification. Activists and policy-makers should take cues from the more radical

elements of the media reform movement (McChesney, 2004), which have worked to build alternative institutional and operational structures based on public service values, rather than the profit model that begets commodification. Again, challenges abound, but examples from the low-power radio movement (Dunbar-Hester, 2014) to Wikipedia (Freedman, 2012) demonstrate the viability of alternative communications institutions and, importantly, show that commodification is not unassailable.

Ultimately, reformers need to broaden their field of vision to account for the problems of commodification, just as radicals must continue to navigate and work to alter the limits of the possible. Future research should consider how the regulatory toolkit might be renewed under frameworks that challenge commodification and the class relations of commercial surveillance. What is certain is that the transparency/consumer empowerment policy frame mischaracterizes the problems it purports to address. Failing to confront commodification and continuing down the current path will almost certainly represent one small step for privacy, one giant leap for commercial surveillance.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Acxiom Corporation (2012) Annual report 2012, 28 May, Little Rock, Arkansas. Available at: http://www.acxiom.com/about-acxiom/investor-information/reports/ (accessed 18 June 2016).

Acxiom Corporation (2013) Acxiom disrupts conventional marketing models with new Audience Operating System (AOS). In: Acxiom.com, 24 September. Available at: http://www.acxiom.com/acxiom-disrupts-conventional-marketing-models-with-new-audience-operating-system-aos/ (accessed 25 August 2015).

Acxiom Corporation (2014) Annual report 2014, 28 May, Little Rock, Arkansas. Available at: http://www.acxiom.com/about-acxiom/investor-information/reports/ (accessed 18 June 2016).

Acxiom Corporation (2016) About Acxiom. In: Acxiom.com. Available at: http://www.acxiom.com/about-acxiom/ (accessed 15 May 2016).

Andrejevic M (2007) *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: University Press of Kansas.

Angwin J (2014) *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York: Times Books.

Ball K and Snider L (eds) (2013) *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. New York: Routledge.

Bamberger KA and Mulligan DK (2011) Privacy on the books and on the ground. *Stanford Law Review* 63: 247–315.

Beckett L (2014) Everything we know about what data brokers know about you. In: ProPublica, 13 June. Available at: http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you (accessed 5 July 2015).

Bennett C (1997) Convergence revisited: toward a global policy for the protection of personal data. In: Agre PE and Rotenberg M (eds) *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press, pp. 99–123.

Brandeis L (1913) What publicity can do. *Harper's Weekly*, 20 December, pp. 10–13.
Brill J (2013) Demanding transparency from data brokers. *The Washington Post*, 15 August. Available at: http://www.washingtonpost.com/opinions/demanding-transparency-from-data-brokers/2013/08/15/00609680–0382–11e3–9259-e2aafe5a5f84_story.html (accessed 5 July 2015).
Bryan D (2013) Acxiom's inaccurate data and why it's so useful. *Direct Marketing News*, 19 September. Available at: http://www.dmnews.com/dataanalytics/acxioms-inaccurate-data-and-why-its-so-useful/article/312329/ (accessed 25 August 2015).
Calvan BC (2012) Data collectors reject assertions they are 'data brokers,' as Congress looks to impose rules. *Boston Globe*, 8 November. Available at: http://www.boston.com/politicalintelligence/2012/11/08/data-collectors-reject-assertions-they-are-data-brokers-congress-looks-impose-rules/uAAffDU9IABHY833eAy6VP/story.html (accessed 25 August 2015).
Cohen JE (2010) The inverse relationship between secrecy and privacy. *Social Research* 77(3): 883–898.
Cohen N (2008) The Valorization of surveillance: towards a political economy of Facebook. *Democratic Communiqué* 22(1): 5–22.
Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011).
Commercial Privacy Bill of Rights Act of 2014, S. 2378, 113th Cong. (2014).
Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (2011).
Consumer Privacy Protection Act of 2015, H.R. 2977, 114th Cong. (2015).
Crain M (2014) Financial markets and online advertising demand: reevaluating the dotcom investment bubble. *Information, Communication, and Society* 17(3): 371–394.
Data Broker Accountability and Transparency Act, S. 2025, 113th Cong. (2014)
Dunbar-Hester C (2014) *Low Power to the People*. Cambridge, MA: MIT Press.
Federal Trade Commission (FTC) (1998) Privacy online: a report to congress, June. Available at: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (accessed 25 August 2015).
Federal Trade Commission (FTC) (2012) Protecting consumer privacy in an era of rapid change: recommendations for business and policymakers, March. Available at: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (accessed 25 August 2015).
Federal Trade Commission (FTC) (2014) Data brokers: a call for transparency and accountability, May. Available at: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (accessed 25 August 2015).
Freedman D (2012) Web 2.0 and the death of the blockbuster economy. In: Curran J, Fenton N and Freedman D (eds) *Misunderstanding the Internet*. New York: Routledge, pp. 69–94.
Fuchs C (2010) Labor in informational capitalism and on the internet. *The Information Society* 26: 179–196.
Gandy OH (2011) The political economy of personal information. In: Wasko J, Murdock G and Sousa H (eds) *The Handbook of Political Economy of Communications*. Malden, MA: Wiley-Blackwell, pp. 436–457.
Harvey D (1982) *The Limits to Capital*. Chicago, IL: University of Chicago Press.
Harvey D (2010) *The Enigma of Capital: And the Crises of Capitalism*. New York: Oxford University Press.
Hicken M (2013) Find out what big data knows about you. *CNN Money*, 5 September. Available at: http://money.cnn.com/2013/09/05/pf/acxiom-consumer-data/index.html (accessed 25 August 2015).

Hoofnagle CJ (2006) Privacy self regulation: a decade of disappointment. In: Winn JK (ed.) *Consumer Protection in the Age of the 'Information Economy.'*. Burlington, VT: Ashgate, pp. 379–402.

Jordan T (2015) *Information Politics: Liberation and Exploitation in the Digital Society*. Chicago, IL: University of Chicago Press.

Koran JF (2015) Some lenders are judging you on much more than finances. *Los Angeles Times*, 19 December. Available at: http://www.latimes.com/business/la-fi-new-credit-score-20151220-story.html (accessed 18 June 2016).

Luxemburg R (1973) *Reform or Revolution*. New York: Pathfinder Press.

McChesney R (2004) *The Problem of the Media*. New York: Monthly Review Press.

McGuigan L and Manzerolle V (eds) (2014) *The Audience Commodity in a Digital Age: Revisiting a Critical Theory of Commercial Media*. New York: Peter Lang.

Maxwell R (1999) The marketplace citizen and the political economy of data trade in the European Union. *The Journal of International Communication* 6(1): 41–56.

Messick G and Gavrilovic M (Producers) (2014) The data brokers: selling your information. *60 Minutes* (Television broadcast), *9 March*. Available at: http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/

Morozov E (2013) Your social networking credit score. *Slate*, 30 January. Available at: http://www.slate.com/articles/technology/future_tense/2013/01/wonga_lenddo_lendup_big_data_and_social_networking_banking.html (accessed 23 May 2016).

Mosco V (1996) *The Political Economy of Communication*. Thousand Oaks, CA: SAGE.

Mosco V (2009) *The Political Economy of Communication*. 2nd ed. Thousand Oaks, CA: SAGE.

Mott N (2014) The FTC condemns the data brokerage industry's collection practices. *Pando Daily*, 27 May. Available at: https://pando.com/2014/05/27/the-ftc-condemns-the-data-brokerage-industrys-collection-practices/ (accessed 25 August 2015).

Nehf JP (2012) *Open Book: The Failed Promise of Information Privacy in America*. Indianapolis, IN: Indiana University Robert H. McKinney School of Law.

Niesen M (2012) The little old lady has teeth: the U.S. Federal trade commission and the advertising industry, 1970–1973. *Advertising & Society Review* 12(4).

Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

Pasquale F (2015) *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press.

Schiller D (1999) *Digital Capitalism*. Cambridge, MA: MIT Press.

Schiller D (2007) *How to Think about Information*. Urbana, IL: University of Illinois Press.

Schiller D (2014) *Digital Depression*. Urbana, IL: University of Illinois Press.

Simon LD (2000) *NetPolicy.com: Public Agenda for a Digital World*. Washington, DC: Woodrow Wilson Center Press.

Singer N (2012) Congress to examine data sellers. *New York Times*, 24 July. Available at: http://nyti.ms/1PyVekO (accessed 25 August 2015).

Singer N (2013) A data broker offers a peek behind the curtain. *New York Times*, 31 August. Available at: http://nyti.ms/1AhMUxK (accessed 25 August 2015).

Smythe DW (1977) Communications: blindspot of Western Marxism. *Canadian Journal of Political and Social Theory* 1(3): 1–27.

Smythe DW (1981) *Dependency Road*. Norwood, MA: Ablex.

Solove DJ (2013) Introduction: privacy self-management and the consent dilemma. *Harvard Law Review* 126(7): 1880–1903.

Stole IL (2006) *Advertising on Trial: Consumer Activism and Corporate Public Relations*. Urbana, IL: University of Illinois Press.

Streeter T (1996) *Selling the Air: A Critique of the Policy of Commercial Broadcasting in the United States*. Chicago, IL: University of Chicago Press.

Tummarello K (2013) Rockefeller: 'Data brokers' worse than NSA spying. *The Hill*, 18 December. Available at: http://thehill.com/policy/technology/193576-rockefeller-data-brokers-worse-than-nsa-spying (accessed 25 August 2015).

Turow J (2011) *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth*. New Haven, CT: Yale University Press.

Turow J, Hennessy M and Draper N (2015) The tradeoff fallacy: how marketers are misrepresenting American consumers and opening them up to exploitation. Report, Annenberg School for Communication, University of Pennsylvania, Pennsylvania PA, June.

US Government Accountability Office (2006) *Personal information: agency and reseller adherence to key privacy principles*. Report no. GAO-06–421, April. Washington, DC: US Government Accountability Office.

US Government Accountability Office (2013) *Information resellers: consumer privacy framework needs to reflect changes in technology and the marketplace*. Report no. GAO-13–663, June. Washington, DC: US Government Accountability Office.

US 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, 18 December. Available at: http://www.commerce.senate.gov/public/?a=Files.Serve&;File_id=0d2b3642-6221-4888-a631-08f2f255b577 (accessed 25 August 2015).

Watson SM (2014) The uncanny valley of targeted marketing. In: saramwatson.com, 11 March. Available at: http://www.saramwatson.com/blog/the-uncanny-valley-of-targeted-marketing (accessed 25 August 2015).

White House (2012) Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy, February. Available at: https://www.whitehouse.gov/sites/default/files/privacy-final.pdf (accessed 25 August 2015).

Whittington J and Hoofnagle CJ (2012) Unpacking privacy's price. *North Carolina Law Review* 90: 1327–1370.

Wright EO (2015) How to be an anti-capitalist today. *Jacobin*, 2 December. Available at: https://www.jacobinmag.com/2015/12/erik-olin-wright-real-utopias-anticapitalism-democracy/

Zuboff S (2015) Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30(1): 75–89.

Author biography

Matthew Crain is an Assistant Professor of Media Studies at Queens College, City University of New York.