Karen Petruska and John Vanderhoef

TV That Watches You:
Data Collection and the Connected Living Room

Abstract

This article examines data collection technologies that power the economics of over-the-top video players, though the relevance of our study extends beyond the living room to all connected devices. After reviewing key moments in which media companies, journalists, scholars, and consumers have publicly debated enhanced mechanisms of data collection powered by digital technologies, we offer a detailed case study of the rhetoric surrounding Microsoft's planned release of the Xbox One gaming console and the Kinect One camera peripheral. We argue that these examples demonstrate the ways corporate media policy evolves through the lived experiences of consumers, with companies struggling to account for broader anxieties over the sacrifice of privacy for the conveniences of technology.

> "'It's like an arms race to hire statisticians nowadays,' said Andreas Weigend, the former chief scientist at *Amazon.com*. 'Mathematicians are suddenly sexy.'"[1]

On a recent episode of *The Good Wife* (CBS 2009 -), teen character Zach Florrick discovers that the camera on his mother's computer has been activated in an empty room (Ep. 5.7, "The Next Week"). Upon further investigation, he learns that the camera on his sister's computer, too, seemingly turns itself on and off, capturing his sister in various stages of undress. While the episode concludes with Zach punching a fellow student whom he suspects of planting spyware to exploit his sister on a naughty Internet site, the program does not examine how Zach puts the genie back in the bottle—i.e. how he removes the objectionable content featuring his sister and prevents its further spread online. Despite the program's easy resolution, *The Good Wife*'s depiction of surveillance technology speaks to wider anxieties about the ways media devices may be looking back at us.

The term "surveillance" carries some negative connotations, particularly for those familiar with Foucault's famous analysis of the panopticon, a mechanism that enforces good behavior through an assumption of surveillance.[2] Notwithstanding, implicit surveillance has long been a key mechanism supporting the economics of broadcasting. Historically, television programming arrived over the air for "free" for Americans who owned a television. Of course, television was never really free, in that sponsors financed television content through the purchase of time, during which they addressed viewers through ads. In essence, the dominant ratings company, Nielsen, surveilled a willing sample audience to extract large viewing patterns that were then commodified through contractual relationships between Nielsen, television networks, and marketers.[3] Increasingly, Nielsen's methods of data collection have required less active participation by its sample audience (recording video information through a box affixed to a television that automatically documents channels selected, for example), and digital

Taylor Nygaard, editor, Spectator 34:2 (Fall 2014): 33-42.

technologies have strongly enhanced the ability of Nielsen and other audience measurements companies to monitor all users of smart devices. This "big data" collection has increased accuracy and enhanced detail for surveillance technologies, but few advances have been made in answering questions about the larger implications for privacy, commerce, citizenship, and the stakes of cultural consumption rendered as data.

Today, smart TVs and over-the-top (OTT) video players arrive embedded with data gathering functionality, and the logics that undergird a business model supported by transforming data about consumer activity into currency has become the dominant framework for the economics of connected viewing.[4] At first, television executives accustomed to a lucrative relationship with sponsors found the economics of web-based content less promising. Thus, even after former NBC executive Jeff Zucker revised in 2009 his initial complaint about digital media economics as an exchange of analog dollars for digital pennies—he declared, "we're at digital nickels now"—the revenue generated by digital media continues to underperform in relation to the advertising rates demanded by old-fashioned over-the-air and cable-wired TV.[5] Media companies have struggled to devise a business model that can exploit big data more fully, and one challenge they face is consumer anxiety about data collection. In this article, we will examine limit cases of media surveillance, including a case study of the Xbox One, to argue that the stakes for media audiences extend beyond convenience to questions of who controls data, who profits from it, and what are the broader implications of a media economy built upon the amassing of vast stores of data about connected viewing.

Netflix and the Failure of Anonymization

Through a quirk of history, federal law has protected media consumption data in a unique manner. After Supreme Court nominee Robert Bork suffered the indignity of the publication of his videotape rental history in a local DC-area newspaper, Congress passed the Video Privacy Protection Act (VPPA) in 1988, which prohibited video stores from releasing customer viewing history.[6] As viewing habits migrated to the web, with 2012 becoming the first year consumers viewed more movies online than on disc, the VPPA became a sticking point for social media and video distribution web sites who based their sites' functionality upon the amassing and sharing of information.[7] Facebook, for example, was sued in 2009 for partnering with Blockbuster to share customer activity. Netflix also struggled with the law's prohibitions, and in 2012 Netflix successfully lobbied to have the law revised to allow consumers to share their viewing data through social media.[8] For twenty years, then, the VPPA protected a consumer's video history through the consumer's right to privacy.

While the U.S. government's National Security Agency recently revealed surveillance tactics provoked outrage among Americans, a *Los Angeles Times* reporter has argued that the data collected and disseminated by companies like Facebook and Amazon reveals more telling details about individual consumers but is much less well understood by those consumers.[9] The amount of that data being collected is also unfathomable: a vice president at IBM Research cited the amount of data circulating globally at a thousand exabytes, or one billion gigabytes.[10] Moreover, the seeming disconnect between NSA surveillance and connected viewing data collection is belied by the variety of ways government agencies employ viewing histories.[11] For example, in his campaign for re-election, President Obama's digital analytics team crunched data collected from Facebook and from set-top box monitoring technology gleaned from cable and satellite companies to pinpoint the exact location of independent voters (and by location we mean the times they would be likely to be in front of the television).[12] Connected viewing data collection has expanded in its scope and intensified in its relevance to a range of stakeholders, but a commitment to protect the consumer's privacy has not increased with equal fervor.

Scholar Mark Andrejevic has rejected the term "privacy" as politically fraught. In his reading of the term, privacy connotes ownership, partitioning space in which the consumer has control. This troubles Andrejevic because privacy therefore depends upon the same logics of private property

that drive the proprietary claims of data companies who collect, package, and sell consumer data.[13] Legal scholar Felix Wu has also questioned the utility of "privacy": "The idea that the term 'privacy' is heavily overloaded is by now well established. It can be used to name a wide variety of concepts, norms, laws, or rights, ranging from the 'right to be let alone' to a respect for 'contextual integrity.'"[14] With so many possible meanings, the attempt to apply the concept of privacy to regulations of big data proves problematic, according to Wu. Consumer motivations cannot be easily reduced to a default openness in all cases.[15] For example, many Facebook users regularly share photos through the social media site, but Facebook's use of those photos in advertisements upset consumers.[16] Debates about privacy, therefore, can serve as limit cases, highlighting our cultural values and the ways they may conflict with commerce. Big data produces value beyond the economic because it captures and quantifies our human experiences. This process is neither banal nor neutral.

Anonymization, the removal or altering of so-called identifiable personal information from data stores, is a strategy employed by media companies to protect consumer privacy. Scholars, however, have repeatedly challenged the effectiveness of anonymization, and a case involving Netflix provides one example. In an effort to improve its movie recommendation system, Netflix announced in 2006 a contest with a prize of a million dollars awarded to the team that most successfully refined the Netflix algorithm. To facilitate research, Netflix released a data set that had been anonymized, but two University of Texas at Austin scholars, Arvind Narayanan and Vitaly Shmatikov, reversed that process by comparing the Netflix data with public IMDB (Internet Movie Database) reviews. The scholars found, "With eight movie ratings (of which two may be completely wrong) and dates that may have a fourteen-day error, 99% of records can be uniquely identified in the dataset."[17] Discussing the Netflix example and other successful efforts by scholars to expose the "spectacular failures" of the anonymization promise, law professor Paul Ohm has argued that data can be "useful" or "private," but not both.[18]

When Edward Snowden exposed the NSA's PRISM program that accessed and stored data derived from emails, video and voice chats, photos, social networking and other digital communication methods, government officials sought to mitigate the scandal by explaining that the agency collected only metadata, or descriptions about media products, not the content of messages surveilled.[19] As with claims of anonymization, journalists and scholars have challenged the notion that metadata is insignificant.[20] A Duke University sociology professor, for instance, published on his website a historical thought experiment through which he proved that the most scant metadata from the time of the American Revolution—the names of colonists and their club memberships—could have exposed Paul Revere as a possible rebel.[21] The professor's larger point intimated that metadata, including seemingly banal information about leisure activities and social relationships, can be exploited by oppressive regimes to limit freedom. Despite these critiques of data collection practices, the extent to which consumers have been anxious about the routine collection of media activity by hardware and software companies is unclear. As reported in *Variety*, a survey from research firm Strategy Analytics found that only 30% of consumers would refuse camera-equipped set-top boxes, with other consumers noting only partial or no concern about the ability of hardware companies to watch over their viewing, gaming, and web surfing.[22]

Then again, some scandals have captured the imagination of consumers by starkly representing the "creep" factor of data collection and marketing strategies. The most infamous example is Target's use of customer purchasing records to identify shoppers most likely to be pregnant.[23] As the story goes, a father complained about Target sending his teenage daughter ads for pregnancy-related products; he later discovered his daughter was indeed pregnant but had not yet told anyone.[24] As the public learned about Target's practices, the company did not stop employing data to market effectively but rather increased the subtlety of its approach by positioning baby items alongside a range of different products to avoid alarming unsuspecting expectant parents. The Target example highlights how seemingly insignificant data, like a record of purchasing unscented lotion and hand sanitizers, may reveal deeply personal

human experiences. In another example, a lawsuit against Netflix over the algorithm contest mentioned above sought damages because the anonymized dataset released by Netflix, and de-anonymized by the UT scholars, revealed that one of their customers was a lesbian.[25] Netflix settled that case and also cancelled a planned second round of the algorithm challenge, and today their data set is one of the most secretive (and prized) within media.[26] Consumers, therefore, may not care about data collection until a scandal reminds them of the extent to which data can create accurate portraits of our interests and values.

The following case study describes in greater detail a more recent example of consumer activism against a media company's efforts to extend surveillance efforts. When Microsoft announced in 2013 the immanent arrival of its latest generation gaming console and over-the-top (OTT) media device, the Xbox One, it also unveiled new requirements of its users to allow a camera peripheral to be continually activated and connected to the Internet. As the case study will detail, consumers and journalists balked, forcing Microsoft to revise its requirements. Despite this seeming success, though, our analysis will offer a more measured analysis of the larger stakes of data collection and connected viewing.

The Xbox One Kinect, or Hal for the Living Room[27]

Dedicated game consoles have transformed into full-service media centers for many households around the world, providing access to a range of media through designated applications. Thanks to the proliferation across devices of OTT apps like Netflix, Hulu, and Amazon, and to the growth of the cable companies' TV Everywhere initiatives, the seventh generation of home game consoles all featured streaming video content options. With the emerging eighth generation of consoles, consisting of Nintendo's Wii U, Sony's PlayStation 4, and Microsoft's Xbox One, video streaming applications are now a central part of the content and marketing package for the hardware.[28] Furthermore, the Wii U and Xbox One have upped their living room commitment by streamlining services that allow a user to access a linear cable feed from the console interface, eliminating the need to switch between the console and TV-watching experience. Hence, despite competition from Roku, AppleTV, and Google's Chromecast, gaming consoles have arguably expanded their utility and become the quintessential connected living room devices. Microsoft's Xbox One in particular features dedicated functions to facilitate TV and movie watching within the Xbox ecosystem. In this section, we delineate a case study of the Xbox One that reveals public anxieties surrounding the future of the connecting living room while at the same time illustrating an evolving connected viewing business model based on trading "private" usage data for the benefit of personalized services and advertising.

Game players, platform holders, and service providers are engaged in a complicated struggle over the personal data of users, inspiring questions about of security, sharing, surveillance, and, broadly, control. In the mobile gaming space, the free-to-play model has normalized data collection as a way to 'pay' for access. Although this model's primary means of revenue is through micro-transactions, convincing players to spend small amounts of money on digital items, many free-to-play games also feature dynamic advertisements, require user registration, and collect valuable user data, sometimes secretly. For example, a lawsuit filed in California in May 2013 accused Google and its third-party app development partners of illegally collecting personal data from Android users, including their geo-location, age and gender, zip codes, activity, and device IDs, among other personal information.[29] Nonetheless, for many gamers the exchange of usage data for access to content has become status quo.

While some home consoles were online in the 1990s, Microsoft was the first to implement a sophisticated data-collection system with its Xbox Live service in 2002. According to their privacy statement, such data allows Microsoft to improve its products, personalize its service, and increase the quality of the gaming experience.[30] With this data, Microsoft recommends games and other media content as promotional blocks through its user interface. According to Microsoft, the company does not share any of the user data it collects with third party developers or advertisers without the

consent of the user. When data security concerns arise, Microsoft tends to fall back on the consent of the user as a crucial element guiding its privacy policies. However, this also pardons Microsoft from having to be responsible for the privacy policies of its publishing and service partners, like Electronic Arts or Flixster, which collect their own data from consumers.

Console gamers received an education in data security when the PlayStation Network (PSN) was hacked in April 2011, compromising the valuable information of 77 million users, including names, addresses, birth dates, and encrypted credit card information. One of the largest data security breaches in history, the hack led to the shutdown of the PlayStation Network service for over a month while new security measures were implemented. To make matters worse, on May 2 of the same year, hackers targeted Sony Online Entertainment, stealing account information from another 25 million users.[31] Members of Congress, journalists, and gamers accused Sony of misrepresenting the enormity of the problem and of unacceptable delay, waiting six days after shutting down the PSN to inform its customers of the breach, leading to at least one lawsuit.[32] Likewise, industry representatives lamented how the attack may have soured consumer willingness to enter the digital ecosystem, while gamers on forums fluctuated between outrage at Sony and the hackers responsible.[33] Nevertheless, consumer anger proved to be temporary and more or less subsided after Sony publicly apologized to its customers ahead of its E3 press conference in June and offered two free PSN games as part of a "Welcome Back" program. Ultimately, the highest price paid by the company was the $171 million the hack ended up costing them. By November 2013 when the PlayStation 4 console sold one million units in its first day of sale, Sony had arguably repaired its public image. From the normalization of data collection to the outrage following the PSN hack, there is a stark but invisible line that demarcates an expectation of a certain degree of "privacy" among gamers, or more accurately, a certain degree of *control* over who has access to their personal information. Leading up to the release of its own new console in 2013, Microsoft, too, stepped up against this line with policies governing the Xbox One.

Microsoft announced the forthcoming Xbox One console and Kinect One camera peripheral at a press event on May 21, 2013. The Kinect One captures video in high-definition 1080p, recognizes up to six unique faces and voices in a room, and can even allegedly detect heart rates by registering subtle changes in skin tone due to capillary swelling.[34] As part of this unveiling, Microsoft explained that users would need to keep the Kinect One camera connected to the console and turned on at all times in order to use the Xbox One for gameplay and other media features. Microsoft also required users to maintain a constant Internet connection so the Xbox One could ping Microsoft servers once every 24 hours in order to prevent hardware hacks and piracy.

After the announcement, critics and gamers expressed apprehension about the privacy implications of an always-on video/audio recording device pointed at the domestic living room. The incomplete nature of Microsoft's initial announcement, coupled with some alarming changes to its existing Xbox 360 policies, caused rumors to go wild within the gaming community.[35] Public reports concentrated on questions of privacy, data use, and security. Could users opt-out of having their data collected by Microsoft, for example? Would Microsoft use the data to create "targeted advertising"? And perhaps inspired by the PS3 hack of 2011, what steps was Microsoft taking to safeguard sensitive data?[36] Many critics called for more transparency and user choice from Microsoft, while others cited the "creepiness" factor as just one of many reasons they were choosing to wait on their Xbox One purchase.[37]

These initial concerns were reignited in early June when NSA documents about domestic spying leaked by Edward Snowden emerged just as Microsoft shared more information about its upcoming Xbox One console leading up to the Electronic Entertainment Expo (E3).[38] Following the deluge of criticism over its initial announcement in May, Microsoft issued a statement clarifying connectivity, licensing, and privacy features for the Xbox One, specifically stating that the Kinect One would not record conversations or send data back to Microsoft cloud servers without a user's permission.[39] However, given the recent NSA revelations, some privacy advocates found the

combination of a networked console connected to the cloud, an always-on camera, and Microsoft's alleged collusion with the NSA to be "absolutely scary."[40] Critics and gamers feared that Microsoft's new console could be one of many connected living room devices incorporated into the NSA's MUSCULAR program that gathered information on millions of people from Microsoft, Google, Facebook, and other media companies.[41] Indeed, among the motivations Edward Snowden ascribed to explain his actions was his worry that the Internet had become "a TV that watches you."[42]

Reflecting the dystopian visions of George Orwell's novel *1984*, Snowden's rhetoric was also adopted by gamers on a Reddit forum dedicated to discussing the Kinect One as an NSA surveillance tool.[43] Members of the gamer community created an array of Internet memes ridiculing the Kinect One as a corporate and government surveillance tool. These images combined other Internet memes with elements from popular culture. One image (see Image 1) riffs on the Russian reversal phrase popularized by Ukranian comedian Yakov Smirnoff, replacing Soviet Russia with Capitalist America, thus ironically juxtaposing the supposed freedom and liberties afforded by laissez-faire capitalism with the mid-to-late 20th century state-controlled Soviet Union. Other images included a picture of the Xbox One and Kinect One accompanied by lyrics from the song "Every Breath You Take" by The Police, including the lyrics, "Every breath you take, every move you make, every bond you break, every step you take, I'll be watching you." Through dozens of memes, the gaming community constructed a language of playful yet pointed criticism aimed at Microsoft's Xbox One policies.

In August 2013, Microsoft announced that the Xbox One would no longer require Kinect to operate, citing demand from consumers.[44] Microsoft's revised policy allowed users to disconnect the Kinect camera completely in addition to deactivating many of its features. Despite this public reversal of company policy, however, Microsoft's rhetoric did not frame the conversation through the issue of privacy. Instead, the company chose a more upbeat perspective by appealing to the ability of the consumer to personalize their Xbox experience. On its website,

Image 1: One of dozens of memes concerned with Kinect One and surveillance

the company offered this short statement about privacy and Kinect:

> You decide how personalized Xbox One is to you and your family, including privacy settings, manual or automatic sign-in, and how data is used. And when you play games or enjoy apps that use sensitive personal data, such as videos, photos, and facial expressions, no one except you can access it, without your express permission.[45]

In the statement, privacy becomes a sub-feature of personalization, a customizable feature rather than a human right. Indeed, Microsoft has packaged privacy as a commodity, one more value-added element of the Xbox experience. At the same time, Microsoft has upheld the relations of power between content providers and consumers, with Microsoft setting the terms. In this case, rather than exchange access for data, Microsoft has promised personalization in exchange for data, a move which seems to be increasingly common in the new age of big data collection and one championed by companies like Netflix.[46] This logic frames data collection as a choice that results in the benefit of targeted, relevant advertisements rather than a violation of trust and personal data.[47]

Microsoft's Kinect technology is merely one of the latest high-profile case studies of the new reality of the connected living room, a media space that promotes convenience, choice, and cross-platform interactions while also exposing home media consumption to serious concerns about surveillance. Consumers are facing increasingly

"smart" technologies, hardware devices that become intelligent through data collection. Thus, consumers must navigate an ever more complex field where technology, policy, privacy, and data interact, where playing a video game or watching TV is no longer just about entertainment but also about fundamental questions concerning the balance between surveillance, personalization, and convenience in the era of the connected living room.

Conclusion

The ubiquity of social media sites have normalized the sharing of personal data, but as companies expand the ways they monetize big data, they may cross an invisible line in the sand that alerts consumers to the possible costs of surveillance. Indeed, as the Xbox One and Kinect One case study illustrates, there are unwritten rules that demarcate acceptable and unacceptable ways to collect and share data. While it seems that line may generally be determined by security failures and other public exposures of the breadth and depth of data surveillance, a lack of established standards guiding companies trying to profit from a range of digital marketing tools suggests not only that similar moments of public anxiety and critical conversation will occur in the future, but also that these are moments during which activists can assert a consumer-centered set of practices that prioritize transparency over secrecy and targeted control over passive consent.

Technology companies who want to monetize user data are pushing the imaginary line of acceptability to normalize ever more invasive collection methods. Incentivizing data collection with so-called "perks" like personalized recommendations and relevant advertisements allows technology and media companies to maintain the public image of respecting privacy rights overall while at the same time benefiting from the ownership and sale of the data. The line is invisible, but so, too, are the transactions that occur when data is aggregated, analyzed, and ultimately disseminated to other companies that benefit from the digital media economy. When consumers sign user agreements, they often exchange rights for access, and only the company is allowed to change the terms at any time without rupturing the contract. Moreover, the "choice" offered to consumers seemingly lies between consent or not participating, and this seems a false dichotomy. Any suggestion that one can "opt out" of the digital data marketplace is naïve at best and fallacious at worst, for true opting out would require a cash economy and access to material media in an age where even libraries have become repositories exclusively of digital content.[48] As such, a more rigorous set of options seems essential to provide consumers with a more agile role in the data economy.

The limit cases examined above demonstrate a powerful but reactive activism. A more proactive discourse may create new understandings of privacy and surveillance paired with a new praxis based around transparency and layers of access, with consumers having a larger voice in determining which companies access particular levels of information and for what purpose. A *Wall Street Journal* article that interviewed experts in consumer rights and data collection explored a variety of possible approaches to the data economy, from the creation of "data copyright laws" and "data profit-sharing" to the self-regulation of media companies choosing not to sell individualized data to third parties.[49] Other options could include web-based media companies simplifying the complexity of user agreements, providing a base level of quality service that prohibits data sharing with any third-party companies, and allowing consumers who would like to opt-out of advertising to pay more for an ad-free experience. The urgent need to define a set of best practices for data collection, storage, and access must extend beyond a limited discourse about individual company policies.

A national solution may be necessary to enforce a consistent set of best practices regarding big data across the wide range of companies with a stake in the economics of connected viewing.[50] Critiques of data collection processes within a recent Senate report and voiced in a speech by the new head of the Federal Trade Commission, Edith Ramirez, suggest that the U.S. government may soon be ready to discuss policies to guide the collection of consumer data.[51] A possible precedent exists in the Fair Credit Report Act, passed by Congress in the 1970s and revised several times

since to extend its consumer protections. As a result of this law, consumers today are empowered once a year to request a free copy of their credit reports from the three major nationwide credit-reporting companies.[52] Furthermore, the credit report includes a list of all companies that have requested access to it. A similar level of access rights may be beneficial for big data, but such a move would require enhancing the visibility of the major companies, like Acxiom, Experian, and Epsilon, currently operating under the radar, who collect, analyze, and disseminate this information.

Wherever the conversation leads, the value of data to a range of stakeholders will maintain its primacy in defining the economics of the digital ecosystem. Data, perhaps even more than bitcoin, is the currency driving the financial lucre of the web, and it seems unlikely that this genie will return to the bottle. Attempts to protect data, through security measures and strategies like anonymization, will fail repeatedly without an equally rigorous partnership extended to the consumers generating the data. The challenge for scholars and critics of such practices is to reclaim a semblance of "privacy"—not by trying to resurrect a historically and culturally specific version of privacy but by redefining the word to acknowledge its complicated existence in an age of connected viewing where privacy is determined by the contrasting discourses constructed around technology, ownership, economics, ethics, policy, and law.

Karen Petruska is the Project Lead for the Media Industries Project's Connected Viewing Initiative at UC Santa Barbara. Her research interests include regulatory policy, digital distribution, and television history. Karen earned her PhD at Georgia State University and has written two book chapters. Her work also appears in Popular Communication, In Media Res, and Antenna.

John Vanderhoef is a PhD candidate in Film and Media Studies at UCSB concentrating on creative labor, video game production, and the boundaries of media industries.

Notes

1 Charles Duhigg, "How Companies Learn Your Secrets," *New York Times*, February 16, 2012. *LexisNexis Academic.*
2 Michel Foucault, *Discipline and Punish: The Birth of the Prison*, Trans. Alan Sheridan. (New York: Vintage Books, 1977).
3 For more about ratings, see Ien Ang's discussion of the "convenient fiction" of the ratings system in *Desperately Seeing the Audience* (New York: Routledge, 1991).
4 For more about over-the-top video applications, see Braun, Joshua. "Going Over the Top: Online Television Distribution as Sociotechnical System." *Communication, Culture & Critique* 6 (2013): 432-458.
5 Chris Albrecht, "Zucker: 'We're At Digital Dimes Now,'" *GigaOM*, March 18, 2009. http://gigaom.com/2009/03/18/zucker-were-at-digital-dimes-now/ (accessed October 19, 2013).
6 Joe Miller, "Congress tweaks US video-privacy law so Netflix can get on Facebook," *Ars Technica,* December 21, 2012, http://arstechnica.com/tech-policy/2012/12/congress-tweaks-us-video-privacy-law-so-netflix-can-get-on-facebook/ (accessed October 19, 2013). For more on the history of the Bork video story, see the author's description of the origins of his story and the fallout: http://www.theamericanporch.com/bork2.htm, and a contemporary news story about the Congressional action: "House Passes 'Bork Bill' Guaranteeing Video Privacy," *Associated Press,* October 19, 1988.
7 Andrew Leonard, "How Netflix is turning viewers into puppets," *Salon*, February 1, 2013, http://www.salon.com/2013/02/01/how_netflix_is_turning_viewers_into_puppets/ (accessed October 19, 2013).
8 Kim Zetter, "Lawsuit Accuses Facebook of Conspiring to Break Video-Privacy Law," *Wired,* November 6, 2009, http://www.wired.com/threatlevel/2009/11/beacon/ (accessed October 19, 2013).
9 Ken Dilanian, "They're Watching Your Every Move: Internet Giants Like Amazon, Google and Facebook May Well Know More About You Than the NSA Does," *Los Angeles Times,* July 10, 2013, A1, *LexisNexis Academic*.
10 Andrew Leonard, "How Netflix is turning viewers into puppets," *Salon*, February 1, 2013, http://www.salon.com/2013/02/01/how_netflix_is_turning_viewers_into_puppets/ (accessed October 19, 2013).
11 Alice E. Marwick, "How Your Data Are Being Deeply Mined." *The New York Review of Books*, January 9, 2014. http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined/?pagination=false (accessed January 9, 2014).
12 Jim Rutenberg, "Data You Can Believe In," *New York Times*, June 23, 2013, *LexisNexis Academic*.
13 Mark Andrejevic, "Watching Television Without Pity: The Productivity of Online Fans," *Television & New Media* 9.1 (2008): 24-46; Mark Andrejevic, "The Work of Being Watched: Interactive Media and the Exploitation of Self-Disclosure," in *The*

Advertising and Consumer Culture Reader, ed. Joseph Turow and Matthew P. McAllister (New York: Routledge, 2009) 385-401.
14 Felix T. Wu, "Defining Privacy and Utility in Data Sets," *University of Colorado Law Review* 84.1117 (Fall 2013).
15 Marshall Kirkpatrick, "Facebook's Zuckerberg Says The Age of Privacy is Over," *ReadWrite*, January 9, 2010, http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov#awesm=~osuZMiJKlRVJEU (accessed January 6, 2014).
16 Kurt Wagner, "How Facebook Is Using Your Photos in Ads." *Mashable*, September 5, 2013, http://mashable.com/2013/09/05/facebook-ads-photo (accessed October 19, 2013).
17 Arvind Narayanan and Vitaly Shmatikov, "Robust De-anonymization of Large Datasets: (How to Break Anonymity of the Netflix Prize Dataset)," Proceedings of the 2008 IEEE Symposium on Security and Privacy May 18-21, 2008, Oakland, California. *LexisNexis Academic.*
18 Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," 57 UCLA Law Review 1701 (2010). *LexisNexis Academic*.
19 Mike Masnick, "Anyone Brushing Off NSA Surveillance Because It's 'Just Metadata' Doesn't Know What Metadata Is," *Tech Dirt,* July 8, 2013, http://www.techdirt.com/articles/20130708/01453123733/ (accessed October 19, 2013).
20 Derrick Harris, "Your metadata can show snoops a whole lot. Just look at mine," *GigaOM*, July 8, 2013, http://gigaom.com/2013/07/08/your-metadata-can-show-snoops-a-whole-lot-just-look-at-mine/ (accessed October 19, 2013); Alexis C. Madrigal, "If It Wasn't the Pregnancy Tests, Why *Did* Baby Catalogs Start Arriving at Our House?" *The Atlantic*, April 18, 2013, http://www.theatlantic.com/technology/archive/2013/04/if-it-wasnt-the-pregnancy-tests-why-did-baby-catalogs-start-arriving-at-our-house/275072/ (accessed October 19, 2013).
21 Kieran Healy, "Using Metadata to Find Paul Revere," *KieranHealy.org,* Personal Website, June 9, 2013, http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/ (accessed October 19, 2013).
22 Todd Spangler, "Surprise: Most TV Viewers Aren't Alarmed by Camera-Enabled Set-Top Boxes," *Variety*, July 8, 2013, http://variety.com/2013/digital/news/surprise-most-tv-viewers-arent-alarmed-by-camera-enabled-set-top-boxes-1200557473/ (accessed October 19, 2013).
23 In a related scandal, Target discovered a data breach (or in their terms, "a payment card issue") in December 2013. "Payment Card Issue FAQ," *Target.com*, https://corporate.target.com/about/shopping-experience/payment-card-issue-faq (accessed January 7, 2014).
24 Charles Duhigg, "How Companies Learn Your Secrets," *New York Times*, February 16, 2012, *LexisNexis Academic.*
25 Ryan Singel, "Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims," *Wired,* December 17, 2009, http://www.wired.com/threatlevel/2009/12/netflix-privacy-lawsuit/ (accessed October 19, 2013); Steve Lohr, "Netflix Cancels Contest After Concerns are Raised About Privacy," *New York Times*, March 12, 2010, http://www.nytimes.com/2010/03/13/technology/13netflix.html (accessed October 19, 2013).
26 Dawn C. Chmielewski, "*Orange Is the New Black* Audience is a Mystery Even to Distributor," *Los Angeles Times*, September 11, 2013, http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-orange-is-the-new-black-audience-shrouded-in-mystery-even-to-its-distributor-20130911,0,4532301.story (accessed October 19, 2013).
27 Hal is the self-aware computer depicted in Stanley Kubrick's film, *2001: A Space Odyssey*.
28 "Game Consoles Marketed as Multimedia Living Room Boxes." *Morning Edition*. National Public Radio Broadcast. November 15, 2013. Transcript available: http://www.npr.org/2013/11/15/245347491/game-consoles-marketed-as-multimedia-living-room-boxes
29 Jaikumar Vijayan, "Google allowing Android app vendors to illegally collect user data, lawsuit alleges," *Computer World,* May 15, 2013, http://www.computerworld.com/s/article/9239253/Google_allowing_Android_app_vendors_to_illegally_collect_user_data_lawsuit_alleges (accessed October 19, 2013)
30 Xbox Privacy Statement, http://www.microsoft.com/privacystatement/en-us/xbox/default.aspx#, (accessed October 19, 2013).
31 Winda Benedetti, "Sony Online Entertainment hacked, some credit card info taken," *NBC News,* May 2, 2011, http://www.nbcnews.com/technology/sony-online-entertainment-hacked-some-credit-card-info-taken-123509 (accessed October 19, 2013).
32 CTV.ca News Staff, "Gamers wonder why Sony took so long to reveal hack," *CTV News*, April 27, 2011, http://www.ctvnews.ca/gamers-wonder-why-sony-took-so-long-to-reveal-hack-1.636743 (accessed October 19, 2013).
33 Keith Stuart, "PlayStation Network hack: industry reactions and theories," *The Guardian*, April 19, 2011, http://www.theguardian.com/technology/gamesblog/2011/apr/29/psn-hack-industry-reactions (accessed October 19, 2013).
34 David Peirce, "The all-seeing Kinect: tracking my face, arms, body, and heart on the Xbox One," *The Verge*, May 21, 2013, http://www.theverge.com/2013/5/21/4353232/kinect-xbox-one-hands-on (accessed October 19, 2013).
35 Some of the changes to its Xbox 360 policies included a requirement that the Xbox 360 console maintain an Internet connection, an aggressive DRM (Digital Rights Management) policy that tied individual games to user accounts so they could not be sold in the secondhand market except through licensed vendors, and as noted in the discussion in this paper, that the Kinect camera peripheral be activated at all times during use of the Xbox One console.
36 Matt Peckham, "Xbox One Raises the Burden of Privacy Safeguards: 5 Questions for Microsoft," *Techland*, May 22, 2013, http://techland.time.com/2013/05/22/xbox-one-raises-the-burden-of-privacy-safeguards-5-questions-for-microsoft/ (accessed October 19, 2013).
37 Brad Reed. "Microsoft's Xbox One policies are driving me into the arms of the PS4," *BGR*, June 7, 2013, http://bgr.com/2013/06/07/microsoft-xbox-one-criticism/ (accessed October 19, 2013).
38 Michael Rundle, "Microsoft Unveils Xbox One Privacy and Digital Rights Details Ahead of E3," *Huffington Post UK*, June 7, 2013, http://www.huffingtonpost.co.uk/2013/06/07/xbox-one-resale-rights-privacy_n_3401119.html (accessed October 19,

2013).
39 Ibid.
40 Chris Miles, "Xbox 1 E3 Announcement: Why It Was So Absolutely Scary," *PolicyMic*, June 11, 2013, http://www.policymic.com/articles/47825/xbox-1-e3-announcement-why-it-was-so-absolutely-scary (accessed October 19, 2013).
41 Barton Gellman and Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say," *Washington Post*, October 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (accessed October 19, 2013).
42 Barton Gellman, "Code name 'Verax': Snowden, in exchanges with Post reporter, made clear he knew risks," *Washington*, June 9, 2013, http://www.washingtonpost.com/world/national-security/code-name-verax-snowden-in-exchanges-with-post-reporter-made-clear-he-knew-risks/2013/06/09/c9a25b54-d14c-11e2-9f1a-1a7cdee20287_story_1.html (accessed October 19, 2013).
43 /r/Games, "With the recent allegations of PRISM and Microsoft, can we trust Microsoft in regards to the Xbox One Kinect sensor and the privacy controls it will provide?" *Reddit*, June 2013, http://www.reddit.com/r/Games/comments/1fygki/with_the_recent_allegations_of_prism_and/ (accessed October 19, 2013).
44 Benjy Sarlin, "Microsoft backtracks on Xbox One camera amid spying fears," MSNBC, Aug. 13, 2013, http://www.msnbc.com/hardball/microsoft-backtracks-xbox-one-camera-amid (accessed October 19, 2013).
45 The Facts, *Xbox.com*, http://www.xbox.com/en-US/xbox-one/get-the-facts (accessed October 19, 2013).
46 Andrejevic, "The Work of Being Watched."
47 T.C. Sottek, "The Xbox One will always be listening to you, in your own home," *The Verge*, May 21, 2013, http://www.theverge.com/2013/5/21/4352596/the-xbox-one-is-always-listening (accessed October 19, 2013).
48 Bill Chappell, "Bookless Public Library Opens in Texas," *The Two-Way* weblog, September 14, 2013, http://www.npr.org/blogs/thetwo-way/2013/09/14/222442870/bookless-public-library-opens-in-texas (accessed December 30, 2013).
49 "Should Companies Profit by Selling Customers' Data?" *Wall Street Journal*, October 24, 2013, *LexisNexis Academic.*
50 While policies exist that allow consumers to opt out of some site's data gathering practices, there is no unified way to establish a prohibition across all websites. "How Hard Is It to Opt Out of Third Party Data Collection?" *Marketplace*, May 22, 2013, http://www.marketplace.org/topics/tech/how-hard-it-opt-out-third-party-data-collection (accessed January 6, 2014).
51 Adam Tanner, "Senate Report Blasts Data Brokers For Continued Secrecy," *Forbes*, December 19, 2013, http://www.forbes.com/sites/adamtanner/2013/12/19/senate-report-blasts-data-brokers-for-continued-secrecy/?utm_campaign=techtwittersf&utm_source=twitter&utm_medium=social (accessed January 6, 2014); Carl Franzen, "New FTC Chief Warns Google, Twitter, big data companies to respect consumer privacy," *The Verge*, August 19 2013, http://www.theverge.com/2013/8/19/4637948/new-ftc-chief-big-data-companies-transparency-speech, (accessed January 3, 2014).
52 The law and its enforcement is not perfect, as discussed in the *Wall Street Journal.* Anna Maria Andriotis, "...Credit Bureaus Won't Tell You," Wall Street Journal, February 17, 2013, ProQuest (accessed January 7, 2014).