J Bus Ethics (2017) 142:71–82
DOI 10.1007/s10551-015-2766-2

Personalized Ad in Your Google Glass? Wearable Technology, Hands-Off Data Collection, and New Policy Imperative

Yong Jin Park[1] · **Marko Skoric**[2]

Received: 5 June 2014 / Accepted: 7 July 2015 / Published online: 12 July 2015

Abstract This study analyzes the increasing presence and capabilities of wearable computing devices in the cornucopia of personalized digital data. We argue that the institutional data practices typical of Google Glass will pose policy challenges and herald yet another dramatic shift to personalized data marketing. We also highlight the characteristics of Google's existing synergetic data practices that will shape the development of not only Google Glass, but also all subsequent wearable mobile devices in light of 360-degree data collection. The key organizing concept of our study is the disjuncture between (1) institutional and (2) policy forces in harnessing dual market mechanism, which frames how the new communication industry operates in the marketplace of ubiquitous personal advertising. We conclude by summarizing the three key areas of political-policy concern (privacy; anti-trust; and user competence) and suggest future solutions, with the discussion on the future of wearable computing practices related to the freedom of the human body.

Keywords Database-marketing surveillance · Wearable technology · Personalization · Privacy · Algorithm-based business model · New media policy

✉ Yong Jin Park
yongjinp@hotmail.com

Marko Skoric
mskoric@cityu.edu.hk

[1] Howard University, 13366 Burikitts Road, Fairfax, VA 22033, USA

[2] City University of Hong Kong, Kowloon Tong, Hong Kong

Introduction

More than 30 years ago, Ithiel de Sola Pool (1977, 1983) noted that the invention of the telephone had greatly enhanced human freedom. Present-day discourse surrounding new technologies remains the same, with smartphones, tablets, smartwatches, and recently Google Glass, all hailed by techno-enthusiasts as tools of human empowerment and freedom. Google co-founder and CEO Sergey Brin declared:

> [Google Glass] is a ultimate future of how you connect with other people.…It frees your hands … your eyes …. and also, frees your ears.

Pool (1983) took great pains to qualify his optimism regarding the new technologies of his day. To him, one of the most urgent tools for realizing their empowering potential is the measured policy option that distinguishes old from new technologies. The premise of Pool's insight highlights the urgent need of the policy imperative to construct new institutional conditions of cultural uses (Pool 1977). In other words, there is the critical need for a shift in understanding among various policy actors—such as the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the Court, and the U.S. Congress—so that they can address unique challenges from new communication technologies that are fundamentally different from the old ones (see Maclaren 2014). There are the two critical interactive factors at play here: (1) the institutional force harnessing the new technologies and (2) the policy response. What Pool (1983) was in fact concerned with was the disjuncture between the two forces, with policy failing to keep up with imminent industry changes.

From this, we put forth the core argument of this study that we are undergoing a dramatic shift toward an era of

wearable computing devices that instigate intensified personalized data marketing and henceforth, should entail clear boundaries that will need to be created by a set of regulations. By policy, we mean broader regulatory principles that condition the operation of commercial institutions in the marketplace (Pool 1983). Specifically, we cover the three related areas of policy concern: (1) privacy and marketing surveillance, (2) anti-trust regulation, and (3) user competence. These are intertwined policy challenges that we identify, as the lack of policy updates since the mid-1990s has exacerbated the data surveillance through concentrated corporate databases. Google Glass is only one of the latest wearable computing platforms that claim human empowerment (cf. Negroponte 1995), but it holds a unique position in the debate. This article stipulates the business and regulatory conditions that are necessary to harness the potential of Google Glass—and other wearable computing devices—as the enablers of human empowerment and freedom.

A wearable computing device is an intelligent machine with built-in computing capabilities that can be worn or attached to a human body. The primary features of wearable computing include not only communicative functions of texting and messaging, but also automated data-mining capacities of a biometric processor such as voice-recognition Siri or Touch ID, as in smartwatches like Samsung Gear and Apple Watch. As tech-policy communities begin to pay increasing attention to wearable computing, we advance the discussion on how to harness policy challenges and on the potential pitfalls that Google Glass and other similar devices may create. Our prediction is that wearable intelligent machines that Google Glass harbingers will become ubiquitous with the intensification of personalization and subsequently, will entail extensive regulation. That is, the success of Google Glass and future wearables as legitimate technological platforms that advance human freedom will hinge upon the development of viable policies that can enable full utilization of its potential.

The present article elaborates this line of thinking by arguing that Google Glass is emblematic of the unique policy challenges posed by the opportunities and the threats of wearable computing devices. In this sense, Google Glass is a symbolic example that should make us take heed of the policy problems of wearable computing technology. We foresee that it is only a matter of time before wearable computing devices become mainstream and the data collection practices of Google are emblematic of what we can expect from the future data practices of other companies. The logical order of the premise, then, is to examine (1) the institutional practices evolving around the new wearable technologies and (2) the existing regulatory contours. This will be followed by the suggestions of policy solutions as the interplay between the institutional and policy factors influences the technological potential (Neuman 1991; Pool 1983). The solution that we are seeking is the nonmarket-based measure of proactive intervention, and we develop this argument by elaborating the failure of hands-off privacy protection, Google's concentrated market power, and the inability of users to protect themselves. In the next section, we first review the industry trends regarding personal data in mobile-based platforms and offer a conceptual framework of institutional data practices and mechanisms, as applicable to the business model of Google and Google Glass. Then, we discuss the key areas of policy and social concern, followed by the future regulatory suggestions.

Google as a Business Institution

Many find it difficult to perceive Google as a profit-driven corporation, and not as a technological innovator that presents search results in an objective and unbiased manner. Previous Pew surveys (Fallows 2005; Purcell 2012) have found that a majority of Internet users have an extremely positive attitude about the information that they gather through Internet searches and trust their favorite search engines; only a few reported that they were aware of the business incentives behind these search engines. Recently, however, we have seen a massive shift in privacy concerns following the revelations regarding the massive NSA data collection program in 2013. In addition, there is new evidence (Park and Jang 2014; Park 2011; Timberg and King 2013) suggesting that the increasing public concern can pressure the companies like Google to modify their privacy policies as many consumers feel uncomfortable with the amount of data collected by businesses and the government, of which the data seizure often happens outside of due process.[1]

To be fair, Google is primarily an advertising-based company to the extent to which its core product, a search engine, is built to maximize user attention and to appeal to its advertisers. In other words, Google offers a search engine in exchange for consumer data, with no direct compensation from users. It aggregates information, filtering out or highlighting information within vast arrays of

[1] In fact, there was a case in which Google challenged a U.S. gag order in order to prevent them from revealing information to the public about the kind of data being collected. This demonstrates how Google is concerned with the public backlash from privacy concern, offering foundation for the argument that corporations can be motivated to address privacy concern to prevent negative PR. As the recent digital landscapes present a potential wakeup call for consumers and spur the consumer movement like Stop Watching Us, the extent of public awareness concerning search engine business practices remains to be explored with a paucity of academic research conducted so far.

the Web universe. In this sense, Google's power lies in its capacity to organize information in such a way as to capture users' attention (Neuman et al. 2012). In short, stipulating Google as an enterprise that commercializes user information according to particular preferences and intentions is an indispensable point of our departure.

Figure 1 summarizes the basic flow of information in Google's business model. The central premise is the duality of the search engine market, which consists of (1) the user market in which the user accesses search queries while locating information and (2) the data market in which the transactions between Google and advertisers are made (cf. Yan and Napoli 2006). This is a peculiar characteristic of a search engine is that users never pay for a commercial product. Rather, the heart of the transaction is in the selling of audience-user data, often done through the auctioning of online search keywords. Nonviewer payment is the characteristic typical of mass media. Yet what differentiates this from the traditional broadcasting model is the extent to which market duality is enabled by data-mining technologies based on an algorithm that tracks, collects, and appropriates real-time user data (Brin and Page 1998; Strickenland 2013). Furthermore, unlike traditional media business models that focus on geographic media buying markets at the aggregate level, the intense commercial transactions of personal data are more likely to center on individual-level profiling, enabling Google and its advertising networks to alter search results and to contextualize and select advertisements according to each user's personal preferences.

Scholars have begun to investigate institutional data marketing practices in relation to political (Hindman 2007), informational (Sunstein 2009), racial (Gandy 2012), and social (Turow 1997) perspectives. Most notably, Danna and Gandy Jr. (2002) analyzed the data-mining surveillance marketing techniques employed in a variety of analytics and database customer relational management (CRM) programs. Their insightful analyses predicted the intensifying trend where numerous firms integrate data points from the Web and other personalized devices to construct a holistic view of their customers. Here the data points may include Web-generated profile information from commercial transactions and from clickstream data. These information sources enable the analysis of shopping cart items, entry and exit points of Web surfing, search terms, and metadata such as a website visitor's location and the duration of the visit (Stead and Gilbert 2001). In fact, this virtually 360-degree view of users has always been a gold mine for digital marketers from the very inception of the product development; it is considered one of the most rational strategies by which marketers infer the best product lines that appeal to particular individuals (Neuman 1991). This pressuring impulse of 360-degree data marketing is what the current and future business models of data-driven companies will aim for. In other words, intensifying market surveillance based on algorithms, as epitomized by Google and its big data, is an embodiment of institutional incentive behind the information-centric economy of personalization.

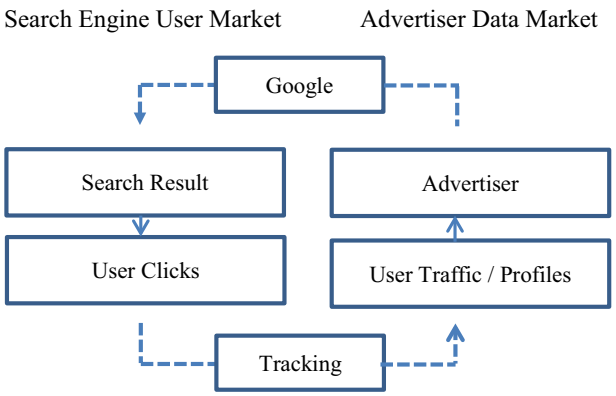

Fig. 1 Architecture of algorithm in the dual search engine market mechanism

Digital Synergy of Google Glass

We suggest that Google's unique market dominance will make Google Glass the central platform for the intensification of data marketing surveillance, and the centerpiece of a trend in which wearable computing devices move to the forefront of the digital transition. Here it is worthwhile to note that Google, with $37.9 billion in revenues in 2013, ranks first in revenues among global media corporations, surpassing such media giants as News Corporation, Walt Disney, Comcast, and CBS. In brief, Google's holdings have vastly expanded horizontally through strategic alliances with various entities, such as private firms, universities, and B-to-B operations, and are tightly connected vertically across more than 25 different Google products. This is a particularly important point because no other Internet company has such a deep 'economy of scope' to capitalize on data surveillance. Google, after all, "wants to read God's mind" (Vaidhyanathan 2012).

Executives in the digital advertising industry often point out that there will be no single path by which Google Glass will emerge in these vast product offerings (Google 2013; Larson et al. 2014). As of 2014, no one had figured out the marketing pathway for this product, including Google itself, and the mass-market success of Google Glass seems a distant dream at this point. There were also incidents in which Google Glass wearers found that they attracted unwanted attention in public places (Wagstaff 2014). In terms of data marketing practices, however, the likely

mechanisms for Google Glass capabilities will set the standards for how other wearable devices will function, with all the techniques in place for a variety of mobile and smartphone platforms. Our projection for digital synergy is multifold: it conjures up scenarios in which data surveillance scales up in domains, such as highly tailored health monitoring of diseases and personalized cloud-banking services integrating all purchase histories, which will bring about unique sets of intensified data marketing practices. Such examples of digital data collection and marketing that wearable devices like Google Glass are likely to intensify will also include

- RFID tracking of the customer movements for retail services through the Google ad network
- Real-time target advertising and personal recommendations in political advertising
- Built-in search engine optimization based on cloud database records
- Embedded location-based service by Google Maps and local weather information
- Instant payment options for commerce and shopping apps (e.g., Google Wallet)
- Biometric data services with voice activations and fingerprint technologies
- Medical data tracking and health profile apps, such as Google lens for diabetes.

This way, wearable computing is poised to be the data-entry point to fuel constant commercial assessments of social, political, economic, and medical background information. Note that the institutional practices at stake are different from data-security issues or illegal data access. Instead, at stake are the scopes of data collection, retention, and appropriation that are perfectly legal under the current regulatory contours (see Turow et al. 2012).

At the infrastructural level, the advancement of wearable computing already has outpaced than that of mobile telephony. On the one hand, the evolution of smartphones or other mobile devices had to undergo the implementation of dependable Internet services (Wasik 2013), while Google Glass can simply tap into the already-stabilized wireless network connectivity to roll out. This enables the vast arrays of institutional platforms that can explore all the data that would otherwise remain commercially unexplored, and brings the power of Google Glass-like wearable devices right in front of users' eyes. In other words, it became possible for all basic data associated with individual users to be processed, integrated, and sold real time in conjunction with other companies—a scale of exploitation that was never possible with a smartphone or mobile telephone. Wearable devices would not be just an extension of conventional mobile technology. With the scope, the intensity, and the locus of data exploitation far beyond what has been practiced before, we do have unique challenges.

In short, Google Glass and future wearables will be designed to encourage active participation, rather than passive or reluctant engagements, in digital data sharing of a 360-degree view, which will accelerate the transition into integrated commercial data services. The operating principle is the same as that for the Google search engine, but vastly expansive in that the search query itself constitutes a de facto opt-in for data tracking and appropriation of customized online ads (cf. Ashworth and Free 2006; Danna and Gandy Jr. 2002). Digital engagement via Google Glass presupposes personal data exposure and personalized mining of physical proximity where the integration of the user's location and data occur with instant real-time availability. This is precisely what stands out from the desktop environment and what data marketers aspire to achieve—namely, a constant feed of real-time location-sensing personal data, combined with capturing of users' bodily movements, to Google service algorithm so as to construct digital identities of targeted consumers (Stampler 2013; Strickenland 2013). Overlapping data points in between platforms can now be tightly connected via Google Glass, embedded in the human body (Google 2013), in anticipation of the perfect match for optimal commercialization (see Fig. 2). Google Glass and wearable computing devices will ultimately enable the selection, maintenance, collection and appropriation of digital trails to get to the very bottom of who you are (in a marketing sense) throughout the lifecycle of synchronized digital experiences.

Figure 3 displays the multiple layers of the extensive data ecosystem within which Google Glass and future wearable Google products will be operating.[2] In the first layer, the core of data mining starts with search queries, with Google dominating more than 70 % of online ad market share. The second layer follows with acquisitions and mergers, such as Google's purchases of DoubleClick, which gave Google the power to link user personal data with third parties, and Waze, which enhanced Google's ability to map and track locational data on each user's movement (Davidoff 2013). Finally, the third layer comes with the continuous expansion of Google's data-mining capabilities through strategic alliances with conventional media companies, such as the New York Times, Amazon, or Disney, which own and deploy their own databases. At the heart of this ecosystem is the data path that goes to and

[2] Here the arrows between Human Body → Google Glass → Google go both ways because that is the nature of Google Glass, which the wearer puts information in, it goes through the cycle, and then winds up back at the human. Likewise, the arrows through "Tracking" and "DoubleClick" are going both ways because all data points in the ecosystem are interconnected, not isolated in individual functions.

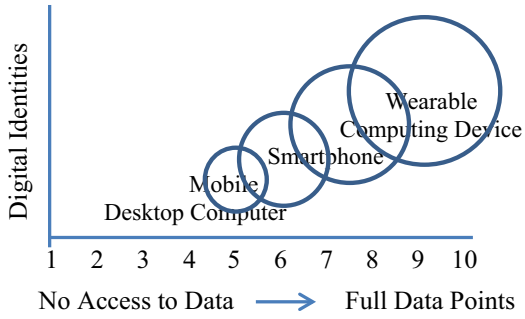

Fig. 2 Data points and scale of digital identities in respective platforms. Scale of digital identities, represented by 360° circle, is bound to increase with more data points

from Google Glass, through which the intensification of data marketing surveillance is enabled by the triangulation of multiple data sources. Note the two aspects of potential data exploitations: (1) directing target advertisements at the precise moment of user movement and (2) retaining, selling, or appropriating personal data for related transactions.

Here it is important to note that Google Glass essentially turns itself into a third-party media company. This means that the traditional media companies could extend via Google Glass to retail environments like Wal-Mart (for instance, a price comparison application or an application that encourages customers to buy complementary products as they shop), or even to local government institutions (for instance, to understand driving patterns or downtown foot traffic patterns). The unique attribute of the wearable devices is the provision of the data-feeding ecosystem instilled at the closest point to a human body. The scale of this ability to compress highly personalized space and moment to seamless data points at the time of precise movements (Campbell and Park 2008) underscores the intensity of data flow created and recreated for commercial purposes. This tight concentration of hardware (Google Glass), software (built-in apps), and associated data-driven companies at the peripheral level results in the data ecosystem architecture that is different from conventional mobile or smartphones with loosely connected layers of platforms, but is built-in to maximize the commercialization of every possible data point. In this way, Google Glass punctuates a tightly synchronized synergy of personal information (Danna and Gandy Jr. 2002; Solove 2001), which is constantly re-engineered and updated by its data-mining algorithm, and engages in entirely new forms of digital data production.

New Media Meet Old Regulation

Ithiel de Sola Pool's key argument was that policymakers at the inception of new media policy "cannot imagine the [technological] changes that lie ahead" (p. 25, 1983; also see Napoli 2001). Thus, there is a disjuncture between what policy is designed to achieve and the challenges posed by new media technologies, that is, much policy deals with the conditions of the present but not the future. This is a critical

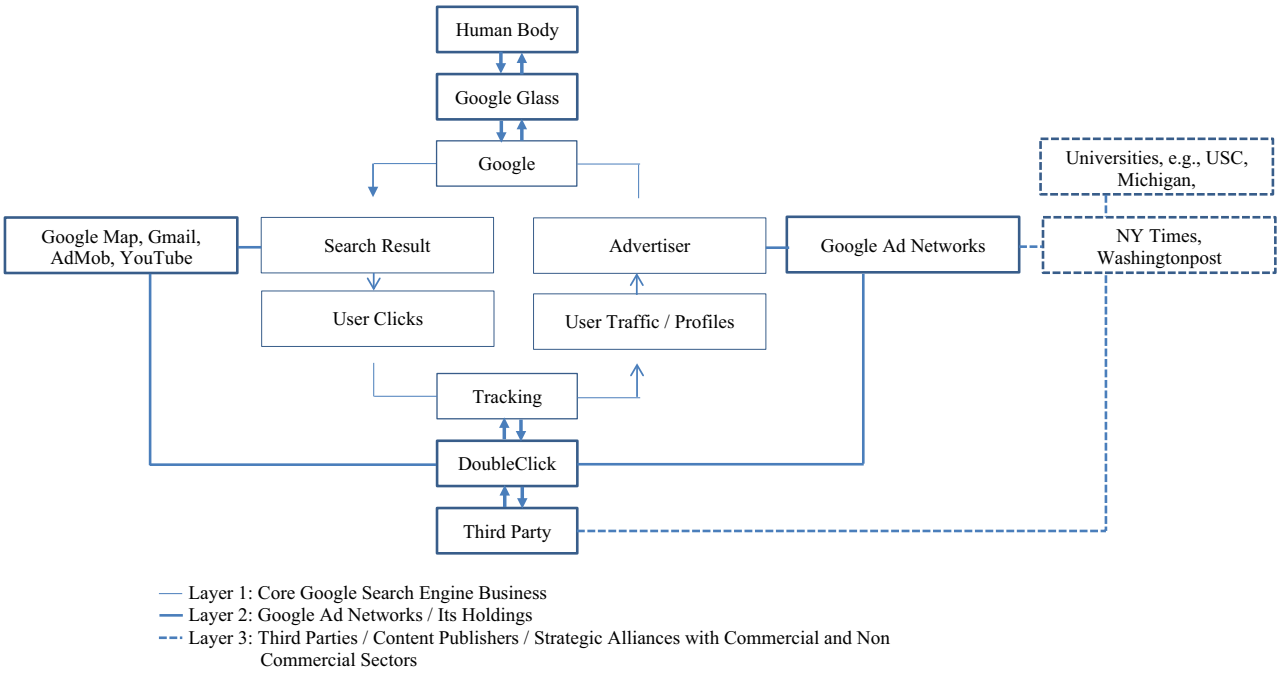

Fig. 3 Google Glass data ecosystem in vertical and horizontal integration

point of our discussion because database marketing techniques such as those that Google Glass is likely to foster are already steps ahead of popular imagination as well as policy understanding. Here we can embody Pool's key criticism that the Supreme Court Justices are often out of touch with technological advancement (see Maclaren 2014). This disjuncture is exacerbated by the Court's long-standing reliance on legal precedent, that is, the past, in formulating its opinions about unprecedented technologies. In this vein, Google Glass epitomizes wearable computing devices that will inevitably necessitate realistic alternatives to the existing policy frameworks and choices based on the Internet-based paradigm of the 1990s.

The hyper-commercialization of personal data that Google Glass and other wearable computing devices will enable in the future is not science fiction. We now live in a world in which our profile data is instantly dissected, contextualized, tracked, and adjusted in real time by digital media buying marketers who constantly optimize the frequency of individual exposure to online targeted ads (i.e., progressive marketing). In fact, Disney World has long used a Radio Frequency Identification (RFID) bracket to track visitors' entry and exit at its theme parks and identify exactly where visitors liked to take their family photos. Years ago, State Farm also infamously installed a speed-tracking device in customers' cars in exchange for insurance discounts so that the insurers could identify the attributes of individual drivers that displayed risky driving behaviors. Digital marketers harbor no secret of the fact that they can follow the online browsing of a pregnant woman, place targeted ads at the right moment, and deliver discount coupons according to her preferences and condition during the nine-month pregnancy.

What is strikingly unique about Google Glass (and other wearable computing devices) is the depth of the interlinked digital data networks through which these tools could provide an unprecedented scale and the scope of seamless personal data integration. That is, a functional equivalent of the supercomputer used to launch Apollo 13 in 1970s will soon be attached to our bodies with numerous sensors, widely open to data marketing exploitations. This is a radical shift away from the desktop computer paradigm in which no personal data was collected as long as the user was physically away from the 'desk' or simply not using the computer. Google Glass therefore sums up the transition from massive data points to a single point of access to real-time data on a human body, all of which can be easily processed and organized into the desired commercial contexts. In this context, great challenges are imminent for policymakers to update the policy that has not changed since the mid-1990s, as in the following three areas of concern: (1) privacy and marketing surveillance regulation; (2) anti-trust regulation; and (3) user competence.

Privacy and Marketing Surveillance Regulation

In the U.S. regulatory context, the digital marketing industry has thrived on a non-interventionist approach since the mid-1990s; the FTC established industrial self-regulation for e-commerce in 1996. Several studies (e.g., Park 2011, 2015a; Campbell 1998; Kang 1998; Lessig 1999) have suggested the ineffectiveness of self-regulation in the online sector. There is evidence that from the very early years online companies in the U.S. did not conform to the standard of voluntary compliance of consumer protection (Notice/Choice) in their website interface design (FTC 1999; Park 2011) and there appears to be no reason to believe that this will change for wearable computing. Google Glass-like wearables provide a critical juncture to ask whether the continuance of this FTC policy stance as well as the lackluster EU regulatory efforts will remain feasible in an age of new wearable devices.[3] This is not to dispute the potential benefits of customization, but to point out that we are in a very different digital environment from the 1990s (cf. Pool 1983), one in which the industry will need a clearer regulatory scope regarding data-mining practices.

Self-regulation regime (of notice and choice), which (1) notifies users and (2) offers an opt-out choice, is inefficient because opting-out will effectively preclude users' engagement in any digital activities. Here the rigid end-user licensing agreement complicates the matter as it prohibits users from altering devices (the hardware or software) for data protection, leaving consumers with very little recourse to choose (cf. Vetter 2006). We do have evidence that suggests data misuse by Internet companies: In the 2013 NSA PRISM surveillance program, the fact that Google also 'pushed' data to the government, in addition to the U.S. government 'pulling' data from the Google database, manifests the enormous power of Google and the government's heavy reliance on private databases, subjecting commercial misuses to even more serious scrutiny. It is imperative that user experience with Google Glass must be equipped with an opt-out option, while opting out should not prevent users from carrying out the functions that default opt-in users would enjoy. Most importantly, the regulatory model should move Google

[3] The criticism of the EU approach was documented in the two grounds: (1) the 1995 EU data directive in the lack of its enforcement power (Robinson et al. 2009) and (2) the 2013 anti-trust battles in which the EU Commission decided to accept Google's proposal (see Kanter 2013). The most recent ruling by the Court of Justice of the European Union concerning 'the right to be forgotten' was also questioned in its vagueness and impracticalities. Still, scholars (e.g., Park 2011, 2013) consistently pointed out the relative strength of the EU principles, as opposed to the self-regulation model in the U.S. where anti-trust charges against Google were dismissed by the FTC in 2013.

Glass and other wearable computing devices toward the opt-in model where the benefits of opt-in are clear and direct.

Anti-trust Regulation

The deeper problem lies in Google's concentration as a business enterprise, which is posited to use Google Glass' combination of massive computing power to monitor and exploit the flow of digital information. Traditionally, the U.S. regulators have focused on horizontal integration in which mergers and acquisitions in media industry occur at the same level of distribution, exhibition, and/or production (Wu 2002, 2011; Yan and Napoli 2006). Yet the vertical concentration of Google raises concerns about how Google's large market power in this unique industry may create entry barriers for small companies hoping to remain competitive in the Glass-like applications market. Google's move to steer away pornographic apps from Google Glass (albeit, a normative concern), for instance, raises fundamental issues about Google's enormous market leverage and what types of apps will be available through small commercial entities. The acquisitions of DoubleClick in 2007, AdMob in 2012, and more recently, Webmaze raise this line of concern because these acquisitions enable Google, not only to mine personal information from vast cross-platforms for consumer preferences and target advertisements, but also to vertically expand deep data sharing within Google's various offerings and strategic partners.

A report suggests that as of 2013, Google commanded as much as 93 % of market share in the mobile ad market, raising the concern of anti-trust regulation in the EU market (Davidoff 2013; Kanter 2013). Likewise, the continuous mergers and acquisitions will leave Google Glass-like wearables as the most, if not the only, viable platforms for small apps to reach target consumers, with applications written for this particular commercial product in its informational needs. Note that Apple in its app market may provide a potentially different scenario as Apple's technological innovation and success hinge upon its cross-platform compatibility, instead of almost exclusively focusing on data collection and use as in the case of Google. The argument here is that the vertical and horizontal contexts of market concentration that Google can potentially leverage through Google Glass will make it more susceptible to the misuse of personal data (Vaidhyanathan 2012). In this regard, regulators have a huge stake in monitoring to ensure (1) that the concentration under the intensive commercialization of data-driven algorithm does not lead to a single consolidation of personal databases and (2) that Google Glass functions as a competitive, if not a neutral, platform for personalized ad markets in wearable computing.

User Competence

It is unlikely that these regulatory measures, no matter how soundly constructed, will be effective without user understandings and skills. In this sense, the most fundamental policy task may be the consideration of end users, that is, "the locus of last clicks" where the entire life journey of digital trails of data points through which database algorithm starts. Evidence (Park 2015a, b) suggests that most online users do not understand online marketing practices and have very little policy knowledge. In addition, despite a relatively high level of privacy concern about cell phones being potentially used to track people's movements, online users do not possess the technical and social skills to protect their privacy. These findings are significant in the context of wearable computing because it is plausible to project that the mobile-based platforms will make it harder for people to understand issues of information flow due to their 'wearability' and 'direct attachment' to human bodies with massive instantaneous data feeding (Campbell and Park 2008).

The deployment of medical apps, such as a heart-rate monitor, calories-intake tracker, glucose monitor in a contact lens, and fitness data, is a cause for concern because the people who utilize these technologies may have an inelastic demand that prevents them from being able to negotiate for their data not to be used. We expect the integration of health data in wearable computing devices to intensify exponentially, partly because of increasing health awareness and technical feasibility. In this vein, another concern may be how underserved user communities will be ready for the transition from desktop-based to mobile and wearable-based computing, as empirical studies display constant stratification patterns of not only access but also use and skill (Hargittai 2008; Park 2015a). In fact, the current FTC and FCC policy have no provision for wearable computing like Google Glass (see Park and Jang 2014). For instance, the FTC in its 2012 update attempted to encompass the regulation of third-party mobile apps in the Children Online Privacy Protection Act (COPPA). Despite some implication of the COPPA for mobile apps, the current regulatory protection for personal identities and location-related application failed to call for any of the user dimensions addressed in this study (see FTC 2012). This lack of references in the latest policy proposal is direct evidence of the incongruence between the regulatory contours and the institutional practices emerging from wearable computing. That is, policymakers need to respond to the emergence of skill disparities in the usage of new technologies and the particular needs of underserved communities (Gandy 2012) as the rapid diffusion of wearable computing devices may

invoke potential pitfalls among those with inadequate skill and knowledge levels.

Paradigm Shift

How would Ithiel de Sola Pool characterize these areas of concern today? It is increasingly clear that the old paradigm of the hands-off regulatory legacy is untenable as wearable computing intensifies the trend in which data marketing surveillance rapidly moves away from the issue of data collection to the intertwined economic and social activities. The specific harms and threats we are projecting are multifold:

(a) The concentration of an integrated data ecosystem that has already begun to raise explicit concerns from the policy (e.g., Davidoff 2013) as well as the scholarly communities (e.g., Vaidhyanathan 2012; Wu 2011);
(b) Data marketing which has been only intensifying privacy violation and data surveillance activities under no due regulatory framework (e.g., Kang 1998; Lessig 1999); and
(c) The lack of user competence in protecting identifiable data, which has been already well documented (Gandy 2012; Hargittai 2008) and can be even more complicated with the increasing level of data transactions through Google Glass-like wearable platforms.

Our example of Google's acquisition of DoubleClick best helps us foresee these potential threats because the merger brought sophisticated data marketing surveillance to Google's vast holdings of data networks and its complex ecosystem about which ordinary users are likely to remain ill informed. Collectively, judging from the use and implementation of past digital technologies, coupled with the economics of the data-driven communication industry, we are not likely to see a move toward fewer concerns regarding wearable computing devices.

These challenges, in our view, offer greater opportunities to update more than decade-old, Web 1.0-based Internet policies concerning privacy, antitrust issues, and user competence. Here the logical path is to narrow the disjuncture between the institutional force harnessing the new technologies and the policy response. This is not only to create effective regulations, but also to predict the trajectory of wearable computing that is still unfolding. On the basis of the impetus behind the institutional practices identified earlier, we can inch policy reconfiguration into a hopeful scenario (Neuman et al. 1993; Pool 1983). Accordingly, a proactive policy frame is proposed to create mechanisms in which policymakers effectively address Google Glass-like wearable computing.

Four Policy Propositions in Summary

The elements of our proposals are as follows: First, vertical integrations within and across new media firms need serious attention from the FTC in order to break the concentration of personal data in digital databases. Second, the user interface in Google Glass and wearable devices should be mandated to contain a function that restricts third-party data access and retention of personal records. Third, there should be a long-term state and local public education campaign for promoting relevant digital skills. Finally, at least in the U.S., Congress should empower the FTC to enact and enforce an updated opt-in model regarding the use of mobile-based wearable platforms.

Along with these suggestions, delicate considerations of cost–benefit analysis are due.[4] While the opt-out model should prevent service or price discrimination from service providers, a desire for service providers to recoup their investment might arise. Likewise, if Google Glass provides users with an ability to block or limit third-party data access, third-party app providers will devise workable compensation schemes by simply charging Google Glass users for full access to their services. This may possibly open a new area of concern on the differentiation between free and paid app services and more fundamentally, on whether a company should be allowed to pressure consumers to give away their data in exchange for being able to utilize services completely. Here careful readers would discern that more nuanced solutions can ensue. For instance, there may be an intermediate approach in which users get compensated for "opt-in" (also see Samuelson 2000). Tort-based solutions (Lessig 1999; Litman 2000) can be based on privacy policy assurance that data would not be associated with the wearer's name. The plausibility of those solutions is worth future considerations for the mutual benefits of users and Google, as the commercial sector has not yet fully adopted such an approach.

The overall premise of our proposal should be perceived as a fundamental principle in which the multiple policy layers in respective functions can generate the benefit for the entire system. The point is that data marketing surveillance protocol can in fact be recoded (Lessig 1999; Sandvig 2007; Wu 2011) with clear government oversight and authority in designing interconnections among

[4] Note the distinction between the institutional privacy, associated with data marketing surveillance, and the social privacy, concerning a wearer's interaction with others in public places. While Google Glass newly disrupts both dimensions of privacy, this study focuses on institutional data practices under formal regulatory policies. This is to be distinct from unwritten social norms that may guide the public–private boundary management of social interactions. Accordingly, the intermediate solutions that we are considering fall into the codified policy areas such as statutes or/and administrative rules.

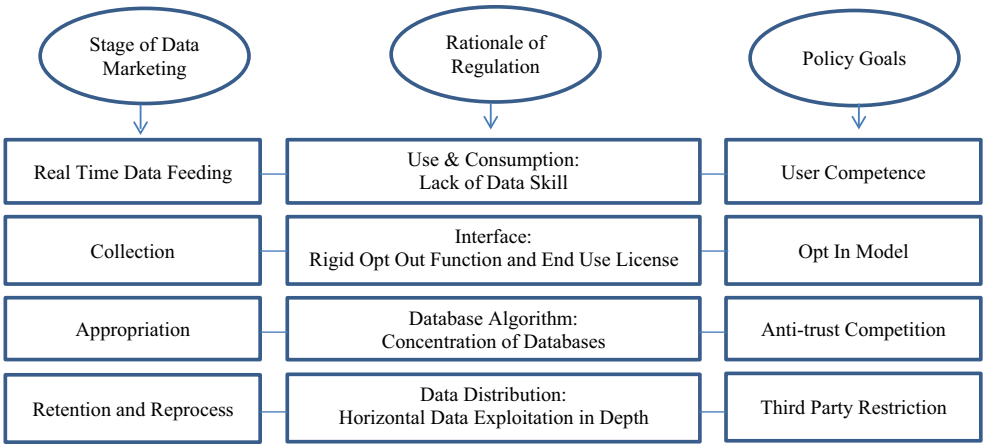

Fig. 4 Layers of policy principle, goals and regulatory rationale in data marketing

different layers of data surveillance as they develop over time. Figure 4 summarizes our policy proposal and rationale with regards to data surveillance marketing. Here each layer of personal data feeding/collection, appropriation, and retention is to have respective policy measures with distinctive goals. This way, the promise of our propositions is built upon the intelligent policy protocol that can guard against unwarranted personal data misuse with the provision of an opt-in choice, as no company would be in a position to abuse its market dominance to create the concentrated private databases that are vulnerable to commercial exploitations of stored data.

In this regard, the FTC will need to have its enforcement power that allows immediate rectification measures once the U.S. Congress gives it the statutory ground concerning data marketing. This is the basic working mechanism behind our proposal—the tighter regulations that set limits on unchecked corporate power and delineate the function of the respective policy layer bearing its own objective. The policy tool that we are arguing is precisely the due enforcement power (that is allocated to the FTC) to translate the policy proposals into the effects they are likely to have. This is a critical shift from the hands-off approach at the heavily concentrated database and inches toward a minimum mandate clause of opt-in interface levels that enable users to exercise data control, with the proactive promotion of user competence allowing the promise of the technology to be realized.

Note that there has been no policy modification concerning data practices in the U.S. since its inception in the mid-1990s. However, Google in its unique market dominance is heralding the rapid advent of ubiquitous wearable computing era. At the least, this contrast between the policy inaction and the rapid technological advancement is the very reason for our concern. The urgency of our proposition is too imminent to miss as we see more and more Google Glass-like devices constructing digital trails tracking people's activity in the home, being able to process and sell their health records, and recording people's eye-gazes at precise points of their life.[5] The reason for our future conjecture is that wearable computing will gain increasingly powerful technical feasibility to engage in data surveillance practices. It is, for instance, logical to perceive a scenario in which an elderly patient relies entirely on a wearable device for instant medical data feedback, but does not understand the complex data surveillance ecosystems and cannot make an informed decision about opting in or out. Less feasible is the argument that the free market mechanism as it is now will solve the problem of the user inability to manage personal data, the gravitation toward concentration in data marketing practices, and the intensification of data surveillance. We have the evidence of the decade-old non-intervention policy approach, which barely alleviated our pressuring concern in the three intertwined areas (Campbell 1998; Vaidhyanathan 2012; Wu 2011, 2012). At the end, we recommend the role of policy in defining the clear objective and scope of institutional behaviors in multiple layers of digital data marketing more than considering its impact on the bottom line (Danna and Gandy Jr. 2002).

Discussion

Evaluation of Institutional Impulse

Our point is not that Google Glass will become a tool of Big Brother. Nor do we argue that privacy should be an absolute point of defense against the hyper-

[5] We fully acknowledge that this critical and insightful point was raised by an anonymous reviewer.

commercialization of personal data. In fact, Google Glass and other wearable computing devices, when structured properly, can be a step closer to enhancing human freedom through its convenience, the integration of services, and the potential functionalities directly attached to individuals' bodies. But the levels of current policy scrutiny, with regard to the dual functions of (1) product/service offerings and (2) personal data marketing surveillance, remain poorly matched with Google's business model, as no measure of regulatory boundaries have ever been perceived for wearable computing devices. This is a cause of our concern precisely because Google Glass will thrive on optimization and customization based on default opt-in for every data point available.

In a bigger picture, the appropriate boundaries that we are proposing are the policy approach with multilayered solutions in which each layer of data collection, appropriation, and retention has respective regulatory measures. The net result will add up so that we can have the opt-in-based wearable platforms, combined with educational efforts and the proactive FTC jurisdiction over database surveillance marketing across digital transactions. A hopeful scenario is that users are aware of the pitfalls related to wearable platforms and can easily opt-in (and out) in the marketplace that is not necessarily integrated into few databases by a handful of companies. Our worst scenario is that a continuous non-intervention approach, for example, in the case of health devices, provides no protection for users whose Google Glass health-monitor data are potentially linked to hinder other transactions, while their decision not to divulge data only means not being able to use the wearable computing services.

Here it should be noted that Google's adherence to the rigid end-user license agreement is predictable in its effort to curtail the potential circumvention of default data feeding. In this regard, the end-user license agreement serves as a basis for informed consent to manipulate the data. Google and the digital data marketing sector will also be quick to point out that any strict regulations would hinder their efforts toward creative digital innovations. This argument, however, precludes a nuanced policy approach that can mutually benefit consumers as well as the industry, and relies on the false premise that the innovation is enabled only by trading personal privacy for a highly concentrated Google corporate structure fueled by a mature digital marketing industry that has in fact benefited from nearly two decades of nonregulation (see Stead and Gilbert 2001).

The important distinction is between the role of Google as a company and the structure in which Google is motivated to harness digital marketing practices. To be clear, our premise is not to blame Google as a single entity with its profit motivation, but to examine the structure within which digital marketing practices are defined and promoted as ideal. It is no longer a secret that the industry perceives data marketing surveillance as the ideal practice to pursue in the digital age. In other words, the hyper-commercialism of marketing surveillance, in which personal data are constantly monitored, collected, and appropriated for the creation of an extensive algorithm-based database, is gaining status as a quintessential norm of legitimate professionalism in the digital marketing sector. Google, after all, will use Google Glass to sell its digital media products to users and sell users to its advertisers -that is, the rational commercial practices that permeate digital media consumption.

It is certainly true that this impulse behind institutional data practices is not unprecedented in a digital platform such as smartphones. Certainly, we welcome a perspective that sees wearables as just an extension of mobile telephone. However, the similarities stopped short, considering that smartphone platforms feed personal data through the loosely connected architecture of independent app-developers and phone manufacturers like Samsung and Apple. Again, the difference is the scale and the intensity of the tight integration that the real-time data collection and appropriation enable at the closest data-entry point of a human body. The linkage is always 'worn' and 'instilled' (as opposed to mobile or smartphones being 'carried') at the human body as it would reinforce the system of data marketing surveillance. This institutional system has been a primary driver of Google search engine success in online advertising and is likely to intensify with Google's institutional impulse to maintain its advantage in wearable computing.

Wearable Computing and Applications

Some industry analysts may argue that Google Glass will be a flop because its high price tag would never allow it to reach a critical mass. The dismissal is the sniff similar to one by former Microsoft CEO Steve Ballmer when he first encountered Apple's iPhone and deplored how 'expensive' such a small phone was. In fact, at the time of this writing, Google Glass (which is still in its infancy) is undergoing the product adjustment to boost its disappointing sales. But that is beside our point. Google Glass, whether or not it succeeds as a commercial product in the marketplace, is likely to continue in other forms of wearable technologies, enhanced and modified by other competitors such as Samsung, Apple, and Microsoft which released HoloLens—its own version of Google Glass in 2015. More importantly, our concern is about the extent to which it will be emblematic of the mobile-based wearable computing devices and associated data collections and whether Google, via its latest venture, will be instigating the policy and social concerns that we already have about Google's overarching dominance in our everyday digital experience.

The recent announcement of health-monitoring mobile apps by Apple and Samsung makes us project one of the most troubling aspects of Google Glass as related to health data. Google already signaled a step in that direction with its Google lens tracking a personalized diabetes level. Beyond the unprecedented algorithm-based data marketing explained above, this raises even more serious concerns about the privacy of medical records as the digital technology attached to an individual person lends itself to the remarkable commercial reach of his or her health profile. We have selected Google Glass to illustrate institutional data practices and policy challenges in a dramatic shift to the era of wearable computing. The parameter of our argument, hence, is not to be bounded by one company's product. Instead, by combining institutional and policy analyses, as well as by closely examining the algorithm-based advertising practices epitomized by Google, our study aimed to construct a clearer picture of the ethical concerns raised by wearable computing in its self-claimed role of promoting human freedom.

Conclusions

It is astounding that the world creates 2.5 quintillion bytes of new data every day, and 90 % of all existing data in the world in 2010 had been created in the previous 2 years (Economist 2010). In this vein, the points made in this work should be punctuated with the expanding role of algorithm-based repositories in storing, organizing, filtering out, or/and commercializing piles of personal information. Note our contention in this paper is beyond the viability of Google Glass. Yet Google Glass-style wearable computing is precisely the technology that will make a data-driven digital life practical to navigate and will thus make us almost exclusively dependent on Google-like intelligence and its commercially appropriated platforms (Neuman et al. 2012). The social viability of Google Glass and other wearable devices will depend on their openness in which users can meaningfully exercise control, contrary to the tight 'black box' model that is integrated for the purpose of intensifying commercialism to encourage consumption based on personalized profiles.

Pool (1983) took pains to elaborate the roles of institutions and culture in shaping the new technologies of his day. Likewise, regulating the institutional conditions of data surveillance will require the operation of Google to include normative objectives[6] on how users' data will be respected. The culmination of our argument is the disjuncture between (1) the institutional imperative of wearable computing conducive to the intensification of data marketing and (2) the regulatory void that safeguards the pressing concern of data collection. We argue that it is possible to narrow the disjuncture by reconstructing the multilayered policy codes ingrained in (existing and future) wearable computing devices which are already outpacing policy imagination. Here the multilayered approach includes opt-in-based platforms that allow users to adjust their access to and retention of data, due regulatory attention on the concentration of digital databases of personal records, and the effort to foster user skills, with the reallocation of FTC enforcement power as a functional mechanism. Yet the fundamental point to recall is that there is nothing intrinsic about the system of digital marketing that is to produce hyper-consumption (selling data) as the system of such massive data surveillance is enabled only by the policy of nonregulation.

[6] See Napoli (2001) who succinctly addressed the long-standing tension in the formulation of communication policies between economic efficiency and normative social objectives.

References

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics, 67*(2), 107–123.

Brin, S., & Page, L. (1998). The anatomy of a large-scale hypertextual Web search engine. In *Proceedings of the seventh international conference on World Wide Web* (pp. 107–117), 14–18 April 1998, Brisbane, Australia.

Campbell, A. J. (1998). Self-regulation and the media. *Federal Communications Law Journal, 51*, 711.

Campbell, S. W., & Park, Y. J. (2008). Social implications of mobile telephony: The rise of personal communication society. *Sociology Compass, 2*(2), 371–387.

Danna, A., & Gandy, O. H., Jr. (2002). All that glitters is not gold: Digging beneath the surface of data mining. *Journal of Business Ethics, 40*(4), 373–386.

Davidoff, S. (2013, June 18). Google's effort to skirt regulation may invite more scrutiny. *The New York Times*, p. B9.

Economist. (2010, February 25). Data, data everywhere. Special Report: Managing Information. Retrieved from http://www.economist.com/node/15557443?story_id=15557443.

Fallows, D. (2005). Search engine users: Internet users are very positive about their online search experiences. Pew Research Internet Project, January 23, 2005.

FTC. (1999). Self-regulation and privacy online: A report to congress. Retrieved from http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-self-regulation-and-privacy-online/privacyonlinetestimony.pdf.

FTC. (2012). FTC strengthens kids' privacy, gives parents greater control over their information by amending childrens online privacy protection rule. Press Release, Dec 19, 2012. Retrieved from http://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.

Gandy, O. H. (2012). *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Farnham: Ashgate Publishing Ltd.

Google. (2013). *What it does—Google Glass*. Retrieved from http://www.google.com/glass/start/what-it-does/.

Hargittai, E. (2008). The digital reproduction of inequality. In D. Grusky (Ed.), *Social stratification* (pp. 936–944). Boulder, CO: Westview Press.

Hindman, M. (2007). "Open-source politics" reconsidered: Emerging patterns in online political participation. In V. Mayer-Schönberger & D. Lazer (Eds.), *From electronic government to information government* (pp. 183–207). Cambridge: MIT Press.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review, 50*(4), 1193–1294.

Kanter, J. (2013, February 1). Google makes offer in 3-year European antitrust case. *The New York Times,* pp. 2, B2.

Larson, J., Glanz, J., & Lehren, A. (2014, January 27). Spy agencies probe angry birds and other apps for personal data. *The New York Times*. Retrieved from http://www.propublica.org/article/spy-agencies-probe-angry-birds-and-other-apps-for-personal-data.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic books.

Litman, J. (2000). Information privacy/information property. *Stanford Law Review, 52*(5), 1283–1313.

Maclaren, S. (2014, June 28). The Supreme Court's baffling tech illiteracy is becoming a problem. *Salon*. Retrieved from http://www.salon.com/2014/06/28/the_supreme_courts_baffling_tech_illiteracy_is_becoming_a_big_problem/.

Napoli, P. M. (2001). *Foundations of communications policy*. New York: Fordham University.

Negroponte, N. (1995). *Being digital*. New York: Knopf.

Neuman, W. R. (1991). *The future of mass audience*. New York: Cambridge University Press.

Neuman, W. R., McKnight, L., & Solomon, R. J. (1993). The politics of a paradigm shift: Telecommunications regulation and the communications revolution. *Political Communication, 10*(1), 77–94.

Neuman, W. R., Park, Y. J., & Panek, E. (2012). Tracking the flow of information into the home: An empirical assessment of the digital revolution in the US from 1960–2005. *International Journal of Communication, 6*, 1022–1041.

Park, Y. J. (2011). Provision of Internet privacy and market conditions: An empirical analysis. *Telecommunications Policy, 35*(7), 650–662.

Park, Y. J. (2013). Offline status, online status: Reproduction of social categories in personal information skill and knowledge. *Social Science Computer Review*, *31*(6), 680–702.

Park, Y. J. (2015a). My whole world's in my palm! The second-level divide of teenagers' mobile use and skill. *New Media & Society, 17*(6), 977–995.

Park, Y. J. (2015b). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior, 50*, 252–258.

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior, 38*, 296–303.

Pool, I. d. S. (1977). *The social impact of telephone*. Cambridge, MA: The MIT Press.

Pool, I. d. S. (1983). *Technologies of freedom*. Cambridge, MA: Belknap Press.

Purcell, K. (2012, Feburary, 2012). Search engine use survey. *Pew Internet & American Life*.

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). *Review of the European data protection directive*. Cambridge: Information Commissioner's Office (ICO), RAND.

Samuelson, P. (2000). Privacy as intellectual property? *Stanford Law Review, 52*(5), 1125–1173.

Sandvig, C. (2007). Network neutrality is the new common carriage. *Info, 9*(2/3), 136–147.

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 53*(6), 1393–1462.

Stampler, L. (2013). Advertisers can't stop thinking about the Google Glass 'pay per gaze' patent. *Business Insider*. Retrieved from http://www.businessinsider.com/advertisers-cant-stop-thinking-about-the-google-glass-pay-per-gaze-patent-2013-8#ixzz2weUtVJvY.

Stead, B. A., & Gilbert, J. (2001). Ethical issues in electronic commerce. *Journal of Business Ethics, 34*(2), 75–85.

Strickenland, J. (2013). *Why is the Google algorithm so important?* How stuff works. Retrieved from http://computer.howstuffworks.com/google-algorithm.htm.

Sunstein, C. R. (2009). *Republic.com 2.0*. New Jersey: Princeton University Press.

Timberg, C., & King, C. (2013, June 18). Google challenges U.S. gag order, citing First Amendment. *Washington Post*. Retrieved from http://www.washingtonpost.com/business/technology/google-challenges-us-gag-order-citing-first-amendment/2013/06/18/96835c72-d832-11e2-a9f2-42ee3912ae0e_story.html.

Turow, J. (1997). *Breaking up America: Advertisers and the new media world*. Chicago, IL: University of Chicago Press.

Turow, J., Carpini, M., & Draper, N. (2012). *Americans roundly reject tailored political advertising at a time when political campaigns are embracing it*. Philadelphia, PA: University of Pennsylvania, Annenberg School of Communication.

Vaidhyanathan, S. (2012). *The Googlization of everything (and why we should worry)*. Berkeley, CA: Univ of California Press.

Vetter, G. R. (2006). Exit and voice in free and open source software licensing: Moderation the rein over software users. *Oregon Law Review, 85*, 183–274.

Wagstaff, K. (2014). Give me your Google Glass and nobody gets hurt! *NBC News*. Retrived from http://www.nbcnews.com/tech/mobile/give-me-your-google-glass-nobody-gets-hurt-n82131.

Wasik, B. (2013, December 17). Why wearable tech will be as big as the smartphone. *Wired*. Retrieved from http://www.wired.com/2013/12/wearable-computers/.

Wu, T. (2003). Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law, 2*(1), 141–179.

Wu, T. (2011). *The master switch: The rise and fall of information empires*. New Jersey: Random House LLC.

Yan, M. Z., & Napoli, P. M. (2006). Market competition, station ownership, and local public affairs programming on broadcast television. *Journal of Communication, 56*(4), 795–812.