Geoforum 42 (2011) 6–15

Contents lists available at ScienceDirect

Geoforum

journal homepage: www.elsevier.com/locate/geoforum

Privacy, reconsidered: New representations, data practices, and the geoweb

Sarah Elwood *, Agnieszka Leszczynski

Department of Geography, University of Washington, Box 353550, Seattle, WA 98195, United States

ARTICLE INFO

Article history:
Received 26 April 2010
Received in revised form 15 July 2010

Keywords:
Geoweb
Volunteered geographic information
Web 2.0
Privacy
Google Street View
Twitter GeoAPI

ABSTRACT

Blogging, social networking, and other Web 2.0 practices have sparked widespread debate about the status and future of privacy. This paper examines an explicitly geographical aspect of Web 2.0 with respect to these debates: the geospatial web, or 'geoweb'. As part of fundamental shifts in the kinds of geographic information available, its circulation, and representative forms it assumes, the geoweb implies new objects of privacy concern and subsequent privacy-related negotiations over the aggregate of its component information, technologies, and data praxes. Thus we argue that privacy must not only be revisited, but indeed re-conceptualized. Whereas prior research on privacy vis-à-vis geographic information technologies has tended to question what privacy 'is', we focus instead on the constitutive outcomes of societal struggles over privacy. We examine how privacy is being negotiated around two geoweb services – Google Street View and the Twitter GeoAPI – to illustrate that these contestations produce privacy as a social object in particular ways. We show that public discourse around actual or anticipated privacy harms stemming from geoweb services and their uses, as well as the preventatives and remedies proposed or implemented to address such harms, reconstitute the objects and practices of privacy concern, and alter the roles and relationships of state, civil and corporate actors in the construction of privacy. Finally we suggest that the geoweb raises new privacy concerns because some of its representational forms – namely geo-tagged images and self-authored texts – facilitate identification and disclosure with more immediacy and less abstraction.

1. Introduction

In *Wired* magazine's 2009 Smart List of ideas for 'changing the world,' one item urged readers to forget privacy, arguing that the social contract over the protection of personal data should be abandoned. Removing the unnecessary obstacle of privacy would, the author argued, enable gains in the speed, precision, and quality of healthcare delivery in the US by facilitating unbounded access to medical information over the Internet (Koerner, 2009). The *Wired* piece is not only a story about healthcare. It is part of a renewed and very public conversation about privacy – its salience, sustainability and desirability – in the age of Web 2.0.[1] Some critics decry the erosion of privacy rights implicated in the posting of intimate details about personal lives online, arguing that this blurring of the 'public' and 'private' compromises the privacy rights of all (Kleinman, 2010; Solove, 2006). Others argue that the loss of privacy is not only inevitable but desirable (Koerner, 2009; West, 2009). These concerns are part of a much larger debate over the role of Internet-based technologies in daily life, and the impact of practices such as blogging and social networking upon social norms, including the protection of privacy.

Here, we focus on an explicitly geographical object of contemporary battles over privacy: the geospatial web, or 'geoweb' (Scharl and Tochtermann, 2007). The 'geoweb' refers to the merging of geographic information with web-based content, often with an implied emphasis on Web 2.0 – based frameworks and services, especially those that emphasize user interactivity and user generation of content. A central practice associated with the geoweb is the 'geotagging' of online content, or the assignation of place names, latitude/longitude coordinates, or any other locational information to text, images, videos, or other Web content.[2] The geoweb consists of hardware (mobile devices), software objects, (applications and services) and programming techniques (such as 'mashing up' content) that include virtual globes, interactive mapping platforms, spatial application programming interfaces (APIs), and technical standards (such as GPX) that guide its curation, aggregation, and dissemination. We use 'the geoweb' here to refer to the constitutive

* Corresponding author. Tel.: +1 206 616 5238; fax: +1 206 543 3313.
E-mail addresses: selwood@u.washington.edu (S. Elwood), agal@u.washington.edu (A. Leszczynski).

[1] 'Web 2.0' refers to the broad series of initiatives and constituent technologies that have redefined the Web away from an assemblage of data repositories (Web 1.0) to a collaborative platform of embedded applications and services of which social networking is a primary example (O'Reilly, 2005).

[2] Geotags may be manually ascribed (user-curated) or automatically generated on-the-fly by applications that run on mobile devices (such as smartphones, WiFi enabled digital cameras, and GPS handhelds).

0016-7185/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.geoforum.2010.08.003

technologies, data, and practices associated with the recent phenomenon of the merging of web content with locational referents.

Geographers' research on the geoweb has coalesced under several additional neologisms, including 'neogeography' (Turner, 2006), 'volunteered geographic information' (Goodchild, 2007), and 'new spatial media' (Crampton, 2009b). An expansive range of issues is considered by this emerging research community, including GIScience questions about digital data handling, data integration and ontologies (Crampton, 2009a; Leszczynski, 2009); methodological questions about techniques for verifying and analyzing the new forms of geographic information that are part of the geoweb (Bishr and Mantelas, 2003; Mummidi and Krumm, 2008); and critical-theoretic approaches to societal impacts of the geoweb upon participation, power, knowledge politics, and privacy (Dodge and Perkins, 2009; Elwood, 2009, 2010; Flanagin and Metzger, 2008; Tulloch, 2008).

Early discussions of the social and political implications of the geoweb suggest that it is part of fundamental shifts in the kinds of geographic information available, the ways that they circulate, and the representative forms they assume. The geoweb is a vector for much broader dissemination of, and access to, locational data, and these shifts are receiving intense societal scrutiny articulated in terms of 'privacy'. In this context, as we will show, actors such as the state and corporations remain central, but the public nature of the geoweb means that new actors and associated data practices are now part of the privacy equation, and that individuals and institutions have new roles and relationships vis-à-vis the production and disclosure of information and identities. Furthermore, whereas past discussions of privacy and geographic information focused for the most part on numerical and text-based tabular data, the geoweb is associated with a tremendous diversification in the modes of representation that we think of as geographic information, including geo-referenced photos, images, videos, narratives, and other artifacts. With all this in mind, privacy must be not only revisited, but re-conceptualized.

It is critical to theorize the privacy implications of the geoweb as more than technologically-driven shifts in access to and dissemination of digital information about individuals, and more than simply the next stage in a progressive trajectory of diminishing control over the release and circulation of information. Of course the representational or communicative capabilities of the geoweb affect privacy, but so too do societal struggles over this new assemblage of socio-technological practices. Thus we begin not from the question of what privacy 'is', but rather, how struggles with regards to spatial information technologies produce privacy as a social object in particular ways. Public discourse around actual or anticipated privacy harms stemming from geoweb services and their uses, as well as the preventatives and remedies being proposed or implemented to address such harms, reconstitute the objects and practices of privacy concern, and in so doing alter the roles and relationships of state, civil and corporate actors in the construction of privacy. Throughout, we also demonstrate that while the reconfiguration of the notion of privacy is global in scope and in reach, the privacy apparatus – the extant legal frameworks, alliances between government and corporations, and their interactions with civil society – operates in diverse ways depending upon institutional and cultural contexts.

These arguments emerge from our analysis of contestations of privacy in relation to two geoweb services: Google Street View and the Twitter GeoAPI. Both services have engendered debates about privacy and surveillance, in the media, courts, and legislative bodies around the world. They involve mass spatial data throughput and provisioning constituted through the geoweb, and as such they shed light on what is 'new' about the social constitution of privacy in this context. Google Street View provides highly realistic visual images of places (buildings, cars, people, sidewalks, gardens, and public gathering places), whereas the Twitter GeoAPI produces geo-tagged snippets of text that can be searched and sorted based on location, or compiled for display on a map. We will argue here that these new forms of representation identify and reveal 'virtual selves' in ways that are more immediate and less abstract than other representations, and their visual nature lends them significant discursive authority.

These cases facilitate several important lines of analysis. Both services are provided by corporations with international reach and are available to users around the world, allowing insight into the ways in which re-negotiations of privacy may occur differently within distinct state and legal structures, as well as the changing role of the private sector in these negotiations. The forms of geographic information circulating through Google Street View and the Twitter GeoAPI rely upon different media, enabling us to consider whether and how privacy is being negotiated differently in relation to the diverse modes of representation that are part of the geoweb. Our discussion of these debates and their implications for the social (re)construction of privacy is based on an analysis of traditional print and online news sources, blogs that host user commentary on new geospatial technologies, and other commentary emerging from lawsuits and new legislation related to these two services.

2. Debating the privacy implications of (spatial) information technologies

Recent studies of the social and political implications of pervasive computing with geo-enabled devices, and of the availability of online high-resolution satellite imagery, hint at the need to consider privacy in light of the geoweb. This literature notes that the technologies, data primitives, and forms of representation that comprise these new phenomena are implicated in fundamental changes to the nature of surveillance, or, more broadly, of seeing: who watches and who is watched, what is seen or revealed, the mechanisms through which this watching occurs, and who has access to the data (Aday and Livingston, 2009; Dave, 2007; Dodge and Perkins, 2009; Perkins and Dodge, 2009). Harris (2006) refers to this transformation as a technologically-enhanced 'occularcentrism', and like Parks (2009), focuses on the ability of geospatial technologies to 'see' where human eyes cannot. Perkins and Dodge (2009) and Aday and Livingstone (2009) emphasize that the geoweb makes it difficult for individuals and institutions to exclusively control geographic information, and suggest a concomitant transformation in the nature of 'secrecy' and strategies used to secure or disrupt it. This perspective builds upon Dodge and Kitchin's (2007) earlier argument that the Internet alters the temporality of concealment and revelation because digital data are accessible beyond the duration of human memory, long after the individuals or conditions may have changed.

These early accounts of the societal implications of the geoweb have largely focused on changes engendered through its constituent technologies and data, such as shifts in how information may be represented, circulated, withheld, or accessed, and by whom; and have then asked what these shifts mean for social and political practice. Such changes in information practices and relationships are intimately related to debates about privacy, yet privacy has been largely unexamined.

But prior research has examined how information technologies (spatial or otherwise) are implicated in privacy and surveillance. Geographers' work in this arena largely emerged from the 'GIS and Society' critiques of the mid-1990s which attended to the privacy implications of: (i) geo-demographic analysis techniques that use inferential statistics to ascribe social characteristics to very small areas based on highly granular data (Crampton, 1995; Curry,

1995a; Goss, 1995a,b), and (ii) very large spatial databases that assemble information about individuals, often without their knowledge or explicit permission, by government actors and private corporations (Curry, 1998; Pickles, 1991).

These authors noted a progressive expansion since the 1970s of both the size and presence of such databases, and a parallel increase in computing power to manipulate these data. They argued that GIS-based spatial databases raise similar threats to privacy as other very large databases (VLDBs) in which individual identifiers such as postal records, IRS records, or credit reports are stored. Spatial databases are especially concerning because data associated with address, latitude/longitude or other geographic information may be assembled to reveal a great deal about people who live at a particular place. Technological advances enable these linkages to be made at unprecedented scales and speeds, with relatively little oversight or regulation. Curry and others further argue that the ability to create linkages across databases on the basis of locational information, first evident in the 1980s, erodes traditional protections of privacy because it effectively reduces individuals to their places of residence ('you are where you live'; Phillips and Curry, 2003).

In these debates, privacy was conceptualized as an individual's ability to control the collection or dissemination of information about him or herself, a boundary that Curry (1998) emphasizes to be historically and geographically contingent. While Curry directly addresses questions of privacy in terms of the erosion of the traditional separation between 'public' and 'private' through geodemographic profiling, most other GIS and Society research did not engage 'privacy' *per se*. Instead, this literature focused largely upon problematic practices, such as surveillance, understood to be enabled by these technologies (Crampton, 1995; Curry, 1995b; Harris and Weiner, 1996; Pickles, 1991, 1995; Sheppard, 1995). Thus the concern was less with the loss of individuals' ability to control information about themselves (privacy), and more with the privacy-eroding practices made possible through geospatial technologies, such as tracking individuals in, through, and from space.

While discussion of the privacy implications and spatial information technologies effectively drops out of postmillennial critical GIS, it persists in urban geography and sociology research. Here, the debate about privacy again emphasizes surveillance, though with a focus on other technologies such as closed-circuit television (CCTV) monitoring (Graham, 1999, 2002, 2005; Graham and Wood, 2003; Norris, 2003; Phillips and Curry, 2003), and practices such as 'dataveillance,' the monitoring of individuals' behavior through mass processing of personal information across institutional and corporate databases (Lyon, 2003; Pleace, 2007; Wood et al., 2007). Like geographers' critiques of GIS and geodemographic profiling, this literature decries the panoptic effects of surveillant technologies and raises concerns about the abstraction of individuals into VLDBs.

The dominant concern of urban geographers and sociologists is the potential consequences of these abstractions, namely the implications of institutions' abilities to construct data assemblages spanning multiple sources. These assemblages are understood to be 'surveillant' in that they facilitate classifying, tracking and monitoring people through databases, and can subsequently structure individual opportunities and life chances (Graham, 2005; Graham and Wood, 2003; Lyon, 2003; Norris, 2003; Phillips and Curry, 2003; Pleace, 2007). Such demographic classifications also produce spaces that reflect the social stratifications inherent in the classifications themselves (Uprichard et al., 2009). The 'social sorting' (Lyon, 2003) that reproduces patterns – and geographies – of social inequality (Graham, 2005). Urban geographers writing on CCTV monitoring focus on the structural selectivity of surveillant practices such as automated facial recognition, rather than documented harms accruing from these practices (e.g. Graham 2005). For example, Graham and Wood (2003) show that automated facial recognition, which involves the real-time matching of persons of interest to their abstraction (in digital photos or video feeds), effectively automates exclusion by targeting already marginalized groups, with consequent reproduction of social inequalities.

These two literatures have identified a host of problematic socio-technological practices related to digital representation, analysis, and dissemination of information. They are invaluable to the theorization of (spatial) information technologies as socially constructed, and have detailed multiple social and political practices in which these technologies are implicated. Yet with respect to theorizing privacy, they are limited in several ways. First, privacy tends to be primarily an entry point, quickly elided to focus on other practices that may result from its erosion or loss: surveillance, structural selectivity, etc. In many of these accounts, what privacy 'is' drops out of view almost immediately, even while remaining central to societal debates at large. Second, a broader examination of privacy is called for because new spatial applications and services associated with the geoweb are more than just surveillant technologies. Surveillance – particularly as conceived in Foucauldian notions of panopticism – implies a unidirectional power relationship between viewers and viewed. Those who own the technology have the ability to track and exert control over the surveilled. As we will show here, the very public nature and unprecedented accessibility of services such as Street View and their digital products complicate this formulation. The geoweb more represents an 'omnopticon' – the 'many surveilling the many' (Rose-Redwood, 2006) – as examples offered by Perkins and Dodge (2009) and Kingsbury and Jones (2009) suggest. Finally, focusing only upon problematic practices that result from a loss or violation of privacy implicitly frames privacy as an end state to be achieved or protected, without examining how the nature of privacy itself is constituted, or may be transformed, through these practices.

If privacy is constituted through social relations as Curry (1998) and others maintain, then resistance or acquiescence to new technology-mediated practices of disclosure, representation, or concealment stand to transform the nature and meaning of privacy itself. This proposition centers our discussion of the privacy implications of the geoweb, and makes broader contributions to theorizing privacy in relation to other information technologies and practices. The question of what privacy 'is', we argue, must be tackled by examining the constitutive effects of social negotiations around privacy.

To illustrate how privacy is being renegotiated vis-à-vis geoweb objects, we examine two popular services – Google's Street View, and Twitter's GeoAPI. These are but two of countless geoweb services, but they have received significant attention with respect to privacy, and thus constitute objects through which we may begin to trace the social (re)construction of privacy through societal responses to the geoweb. We examine what these services do and describe the public debates that have ensued, drawing out the actual and anticipated privacy harms that have been articulated or claimed, and the interventions and remedies proposed and implemented. Subsequently, we show how these debates and interventions are linked to changes in the roles and responsibilities afforded to state, civil, and corporate actors with regard to privacy. This serves to illustrate how changes are being wrought in conceptualizations of what privacy is; the nature and functions of the 'privacy apparatus' of state, citizens, and the private sector; and the solutions sought and proposed for handling privacy in this new environment.

3. The worldwide woes of Google, Twitter, and others

Google Street View and Twitter's GeoAPI are two widely-used geoweb services. Google Street View, released in the US in 2007,

consists of high-resolution digital images captured by cameras mounted to a vehicle that scans images of cities (and to a lesser extent, rural areas) at street level as it drives along their road networks. Because these scans are taken at ground-level, they capture individuals and vehicles in the scene. Persons walking down the street when the Google vehicle passes by inadvertently become part the 'street view' that is disseminated via the Google Maps or Google Earth platforms. In these platforms, a user can zoom from an overhead air photo or planimetric map view to Street View (if it is available), where individual bodies and objects such as cars, houses, and gardens are clearly identifiable.

Initially Street View imagery was released in its 'raw' form, but today the imagery is subjected to a series of algorithms that automatically blur – or pixilate – faces and auto number tags (Paul, 2009a; Shankland, 2008; Siddique 2009). The results of this blurring are demonstrably unreliable, returning 'false positives' such as a Canadian case where Colonel Sanders' visage on a KFC restaurant sign was pixilated, while the faces of actual passers-by remained clearly visible (Schmidt, 2009a, 2009b). Other incidents are less comical, including Street View images depicting persons engaged in private activities that transgress social taboos, such as a highly publicized Swiss case of a politician falsely accused of having an affair when he was 'caught' in a Street View scene walking with a woman later revealed to be his secretary (Klapper, 2009; Rodrigues, 2009).

Twitter's GeoAPI also raises privacy concerns, although these are different in nature. This service allows users of Twitter's microblog service to automatically attach their location to posts, or 'tweets' (Cohen, 2009; Crowe, 2009; Fee, 2009; Letham, 2009; Paul, 2009b; Sarver, 2009; Schutzberg, 2009). Through such geotagged tweets, the user's location is revealed to others, and can be geovisualized in a map. Interestingly, Google's mapping platforms are often used for such mashups. Because Twitter's microblogging service is premised upon systematic user updates throughout the day, the new GeoAPI allows individuals to be identified at their precise locations at any point in time, apprising other users of changes in their status on-the-fly.[3]

The Twitter GeoAPI and Street View both potentially reveal individual or personal information, but they differ in the temporality and visual form of their representations. Street View images are not released live, and may be assembled from multiple images collected at different times. Twitter's service is not only 'real time', but enables collection of location-stamped points comprised by the aggregate of a user's tweets over time, a rich data source from which to reconstruct spatial histories and mobilities. With respect to their visualization capabilities, Street View releases photographic images, a sort of 'primary' visual data, whereas geo-tagged snippets of text from Twitter that appear in a map mashup are a sort of 'secondary' visual representation – they are not visual media in the original form in which they were collected. The services differ in other ways that we will discuss below, such as their approaches for regulating the collection and release of personal information.

A variety of concerns have been raised about the consequences of these geoweb services, related to what is represented in the information released, problematic uses of it, and oversight of information practices. The photographic nature of Street View images enable reproduction and dissemination of evidence (or assumptions) of stigmatized or potentially embarrassing behavior, as in the Swiss case and others (CNN, 2009; Rodrigues, 2009; Weaver, 2009). The uncurated nature of user-generated geographic content is also a source of concern, given that users may identify other individuals and make harassing or disparaging remarks about them, true or not. A prime example is the now-defunct RottenNeighbor.com, a Google Maps mashup in which users ranted about the poor behavior of neighbors, often attaching blatantly discriminatory or stereotypical comments to the purported offenders' home locations. The release of this kind of individual information with a geographic component can introduce new socio-spatial vulnerabilities, as argued by the creators of a recently-released web service, PleaseRobMe.com, which aggregates the tweets of users who broadcast their real-time locations. They contend that users who indicate that they are away from home unintentionally notify potential burglars of this fact (The Economist, 2010). Such risks may seem far-fetched, but the aggregation of geo-tagged tweets does raises other problematic possibilities, such as the ability to identify a person's regular pattern of movement and use such reconstructed spatial histories for stalking or harrassment.

Societal concerns about geoweb services have been articulated largely in terms of privacy. Google Street View has been at the center of the storm. The saga of privacy challenges to Street View begins in the United States, where Google first introduced this service in 2007 (Paul, 2009a; Siddique, 2009). In a civil law suit (*Boring vs. Google*), a Pennsylvania couple claimed invasion of privacy when Google trespassed onto their property to image their home and the road leading to it (Kiss, 2009; Perez, 2009; The Smoking Gun, 2008a). The plaintiffs sought damages associated with lowered property value, claiming privacy was intrinsic to the value of their home, because of its seclusion on a private road. This virtual revealing of their property, they argued, made their house 'accessible,' thus diminishing its latent value (Raphael, 2009; The Smoking Gun, 2008a). The judge dismissed the case on the basis that the plaintiffs failed to ask Google to remove the photographs, and that they had released the address of their property to the public by filing suit. In the latter act, the judge reasoned, the Borings effectively violated their own privacy, preventing them from holding another party to a separate higher standard (Kiss, 2009; Perez, 2009).

In the US, there is no state body charged with privacy or data protection, so such contestations tend to originate from civil society and occur within the legal system (Solove, 2006). The *Boring vs. Google* suit is by no means the sole subject of legal actions over locational privacy currently before US courts[4], yet it is a telling indication of the ill-preparedness of existing legal frameworks to grapple with the new modes of representation that are part of the geoweb. Pomfret (2010) has argued more broadly that Google's information practices are being regulated in an environment of anachronistic and outdated legislation scripted before the rise of the Internet.[5] Countless recent cases evidence this situation, including recent concern about the collection of passwords, emails, video and audio from unsecured wireless networks, as Street View vehicles drove through cities around the world (BBC, 2010a,b,c; Reuters, 2010; Shiels, 2010a). While such practices do not violate individuals' privacy by systematically recording their *location* in a public place (Blumberg and Eckersley, 2009), personal information was clearly gathered without notification or permission. This practice may violate the pri-

[3] A number of other geo-social networking services, such as Loopt or Four Square, provide similar services.

[4] For example, in 2009, the American Civil Liberties Union (ACLU) and Electronic Frontier Foundation (EFF) challenged the FBI's warrantless use of GPS to track the movement of individuals in narcotics cases (see *US v. Jones*, also Electronic Frontier Foundation, 2009; Goodin, 2009; Scarcella, 2009). Such warrantless GPS tracking has been ruled unconstitutional in New York and Massachusetts (Frank, 2009).

[5] For example, the US Electronic Communications Privacy Act was passed in 1986 and as such does not cover new (spatial) media artifacts such as emails, text messages, or GPS pings. The 'Digital Due Process Coalition', which includes companies such as Google and eBay, is campaigning for updates to the Act (Shiels, 2010b). Further, at the time of writing, a draft Internet privacy bill introduced by Congressmen Boucher and Stearns calls for advance notification when individuals' information is beings collected and/or disseminated to third parties, such that they may opt in or opt out.

vacy laws of upward of 30 countries, and has sparked several civil lawsuits and a multi-jurisdictional investigation in the US (BBC, 2010b,c; Reuters, 2010).

Institutions in multiple jurisdictions have already deemed that Street View – the Wi–Fi scandal notwithstanding – *does* violate privacy in location-specific ways. These challenges have primarily centered upon the ability to identify individuals through facial characteristics or license plate information. Japan's Ministry of Internal Affairs and Communication conducted a probe after citizen complaints about malicious secondary uses of Street View images to harass individuals (Williams, 2009; Zafra, 2009). Canada's Office of the Privacy Commissioner and Parliamentary Standing Committee on Ethics, Privacy and Access to Information undertook a lengthy assessment of Street View's legality on the grounds that imaging occurred without prior individual knowledge or explicit consent (as required under Canadian law), delaying the release of Street View by up to two years (Schmidt, 2009a; Wong, 2009). Street View's entry into the UK was also postponed as the Information Commissioner assessed potential impacts under the Data Protection Act (Cross, 2009; Harris, 2009a; Paul, 2009a; Weaver, 2009). The Hellenic Data Protection Authority completely censured Street View in Greece while it sought more information and privacy assurances (CNN, 2009; Haines, 2009a; Paul, 2009a; Rodrigues, 2009; Smith, 2009; Siddique, 2009). In these European cases, Street View has also been subject to data handling guidelines set by the EU.

While many of these disputes are in progress at the time of writing, diverse outcomes and responses are already evident. Japan stipulated that Google re-image the entire country using altered techniques for capturing the images, along with a requirement to notify residents in advance (Haines, 2009b; Paul, 2009a; Williams, 2009; Zafra, 2009). The UK Information Commissioners Office received hundreds of individual complaints in the aftermath of Street View's roll-out, yet continues to deem it legal, citing the *a priori* presence of other privacy-eroding technologies (Cross, 2009; Weaver, 2009). This logic is similar to the justification provided in *Boring vs. Google*, but the state is taking a very different role in the constitution of privacy in each context. In the UK, the state (in the form of an agency charged with the oversight and protection of digital data) retains a presence in the negotiation of privacy through it own established (spatial) data governance regimes. In the US, the state (in the form of the court system) reaffirms the notion of privacy as a relationship between individuals and information collectors such as Google, and tacitly refuses to take a regulatory role. The geographic contingency of the privacy apparatus is also evident in Google's varying response to demands from state actors. When the Swiss Federal Data Protection and Information Commissioner demanded a re-imaging of its streets, as was done in Japan, their request was refused (BBC, 2009; Capper, 2009; Haines, 2009b; Kirk, 2009; Klapper, 2009).

These debates about Street View have centered in part on Google's information-handling approaches, especially with respect to gaining consent, preventing pernicious uses of released information, and stipulating the form or content of the information that is released. In some instances, these preventions and remedies stem from corporate actors' own practices or policies initiated in response to privacy concerns, and in others, from the accommodations requested or imposed by civil and state actors. These practices are thus part of a reconstitution of privacy rendered through social struggles over the privacy implications of new technologies and their modes of representation, communication and analysis.

At present, two principle kinds of solutions or approaches to privacy concerns on the geoweb are in play – *agent-centered* and *technology-centered* remedies. Agent-centered solutions are approaches in which the onus is on an individual (usually civil) actor to take some action related to the release or withholding of information. Street View and Twitter both include agent-centered approaches, albeit in different ways. Individuals who do not wish to be included as part of a Street View image frame must request image removal through Google's 'Report a problem' widget – an 'opt-out' approach. In contrast, Twitter's geotagging functionality is disabled by default. Users must 'opt-in' to the service by intentionally modifying their account settings to allow the annotation of blog entries with spatial referents (Crowe, 2009; Krikonian, 2009; Paul, 2009b; Sarver, 2009; Trapani, 2009). Both approaches are premised on the intentional actions of agents, yet one requires users' knowing enrollment in a service that discloses their spatial position, while the other is based on intentional self-exclusion from a service that has already disclosed information. Twitter's direct solicitation of users' consent to broadcast their locations over the geoweb, we suggest, is one reason why it has not generated the same resistance as Street View. An opt-in approach obviates the potential for lawuits like *Boring vs. Google*, since an individual who knowingly enabled a feature disclosing his or her location has little ground to claim infringement upon his/her right to privacy.

The other common agent-centered approach has been foisted upon geoweb service providers by national states. In several countries, including Japan and Canada, Google is now required to make public notification to residents prior to imagining (Schmidt, 2009a; Wong, 2009; Zafra, 2009). More broadly, the Street View website itself discloses where its vehicles are collecting imagery.[6] Efforts to announce the collection of imagery are an agent-centered approach to information handling at two levels. First, they require geoweb service providers to take some action to help prevent privacy harms. But further, these approaches *also* put the onus on individuals to take action based upon such public announcements. Providing information to the public about what areas will be imaged and when is presumably done so that individuals can absent themselves, or obscure objects and refrain from activities they do not wish included in Street View imagery.

In contrast to the above approaches, a number of *technology-centered* approaches intervene at the level of technology to alter the nature or availability of information that becomes part of the geoweb. One approach involves *scalar shifts* or *spatial offsets,* such as lower camera heights. The Japanese government stipulated that the entire country be rescanned with camera heights lowered from 2.45 to 2.05 meters, on the basis that the original position could capture more than was visible to the human eye, thus 'seeing' past physical privacy barriers such as garden walls (Brandley, 2009; Haines, 2009b; Paul, 2009a; Rodrigues, 2009; Williams, 2009; Zafra, 2009). *Scalar granularity and aggregation techniques* include practices that dither or decrease the resolution of data, such as the blurring or 'fuzzing' of sensitive objects, as in Street View's blurring of faces. These techniques are also applied to places. For example, the US, South Korea, and China have called for obfuscation of military or other sites of national security concern on satellite imagery disseminated through Google applications, either by manipulating the resolution of parts of an image or replacing high-resolution imagery with lower-quality data (Blamont, 2008; Crampton, 2008; Nourbakhsh et al., 2006; Zook and Graham, 2007). Lastly, we find *time-sensitive data handling* describes approaches directed at privacy violations that could accrue from the indefinite retention of data. Twitter, for instance, automatically strips geographical location from all posts after 14 days, permanently deleting spatial information from its own databases.[7] Time-sensitive data handling

[6] http://maps.google.com/help/maps/streetview/where-is-street-view.html.

[7] Some commentators suggest this action is motivated not by an overwhelming interest in protecting privacy, but in preempting lawsuits over subpoenas for users' locations (Trapani, 2009).

has also been imposed, as in a recent EU mandate that Google delete raw Street View imagery from its central data repositories after six months (White, 2009). Canada makes a similar requirement, on the grounds that the indefinite retention of personally identifying information by corporations may violate privacy (Meller, 2008; out-law.com, 2009; Schmidt, 2009a; Wong 2009).

This plethora of government-initiated privacy investigations of geoweb services, and the copious coverage in traditional and new media sources may beg the question of how concerned individual citizens are about potential shifts in privacy, and whether the current uproar is simply being perpetuated for media gain. To these points, we note that most of the government challenges discussed above were initiated in response to citizen complaints. Further, the blogosphere is rife with individuals expressing a newfound concern over *spatial* privacy specifically (for example, see commentary from Madden (2009) and Hyde (2010)). Other direct forms of resistance by citizens are evidence, as in the British village of Broughton, where residents blockaded streets to prevent Street View vehicle from entering the village, expressing fears that imaging of citizen property would aid burglaries (CNN, 2009).

But more broadly, we argue that struggles over privacy are constitutive regardless of the volume of challenges or whether they emerge from media, government, or citizen action. We see today a variety of concerns raised about privacy with respect to the geoweb, and regulations and proferred remedies emerging from the negotiations of civil, state, and corporate actors over the geoweb and its new information and practices. Yet five years after the ascendence of the geoweb, what is new or different about privacy, as a result of these machinations? In the next section, we turn to this question.

4. Reconstituting privacy over the geoweb

The negotiations of state, corporate and civil actors about the geoweb are actively transforming privacy with respect to information: its meanings, socially-constituted understandings of reasonable expectations for it, and practices used to foster or protect it. To the elusive question of what privacy 'is', we submit that in this context, privacy is socially-mediated expectations about acceptable practices with respect to *access* to geographically-indexed information, its *disclosure*, and its *content* and *medium* of its representation when released. What privacy is remains important; it certainly matters whether (and where) privacy is understood as a social contract, or a legal entity, and what its substance or boundaries are understood to be. But the more interesting question for social scientists is not what privacy *is*, but rather, what societal negotiations over privacy *do* to rework the objects of privacy concern and the roles and relationships of actors involved in information production and disclosure. Struggles over privacy and the geoweb are transformative in both realms – they constitute new objects of privacy concern, and reconstitute the roles and relationships of civil, state, and corporate actors in the creation, release, and withholding of information.

4.1. New objects of privacy concern

The furor over privacy with respect to Google Street View, Twitter's GeoAPI, and other geoweb services bring to the fore new objects of concern. In the harms claimed or projected, and the ameliorative measures taken or proposed, the objects of concern are geo-located media that may reveal the presence or activities of individuals at specific places. In the case of Street View, these media are photograph-like digital images, and on Twitter, they are self-authored texts that carry spatial and temporal attributes. A central focus in these privacy debates is the *nature of identification* and *representation* within these geo-located media, and these debates reveal that something different is at stake in the geoweb than in prior privacy debates over very large databases, GIS, or geo-demographic systems.

The nature of identification refers to the ways that identity is incorporated or produced. For instance, credit scores provide an abstracted measurement of a person's actual borrowing and payment behavior. In contrast, an image in Street View may provide a visual reproduction of a person's presence and *perhaps* his or her behaviors at a given location. Inextricably wrapped up with the nature of identification is the nature of the representation – the media through which this identifying information is imparted. The identifying information may be disclosed in the form of a visual representation (such as a photograph or a map), a textual account such as a Twitter post, or tabular attributes, as in the case of the information found in a credit agency's database or a GIS-based attribute table.

Different modes of identification and representation raise varying concerns with respect to privacy for two reasons: they carry differing discursive authority and they operate at different levels of immediacy and abstraction. To the first point, visual forms of information are more likely to be accepted as 'true' or 'accurate' than others. Many of the concerns leveled at Street View stem from situations where its photograph-like images were treated as definitive evidence of an individual's involvement in particular activities. The visual nature of these pseudorelistic images, as well as the fine scale and resolution of the imagery itself, lead to them being taken as 'truth', consistent with longstanding Western philosophical traditions that equate seeing with knowing, and visual epistemologies with objectivity (Crang, 2003; Daston and Galison, 2007; Rose, 2007; Ryan, 2003; Sui, 2000; Tuan, 1979).

The degree of abstraction or immediacy with which this knowing may occur is a further concern, particularly the greater immediacy of the geoweb when compared to prior spatial information technologies. Representations exist at differing levels of abstraction or immanence, requiring different degrees of intervention in order to discern who is doing what, where, and when. For example, re-associating information with individuals based on spatial identifiers, a key object of concern in privacy debates about very large databases and GIS, requires significant further processing of information abstracted from the individual. In contrast, the ability to identify individuals with imagery from Street View is imminent to the representational form itself, rather than based on the possibility of geographical association through spatial linkages across databases or reverse geocoding. The ability to geovisualize a person's presence in or movements through space from text geotagged with Twitter's GeoAPI is not immanent to the representation itself, but rather would require additional steps, such as rendering the tweets as points on a map mashup.

We submit that contemporary privacy debates about the geoweb are spurred by the immediacy and directness of its identification and representation of virtual selves. In Google Street View, this virtual self exists visually, present in the form of bodies captured in Street View images, or artifacts assumed to stand in for the presence of the person – houses or vehicles. In geo-tagged tweets, this virtual self is embodied in spatially- and temporally-situated text released by the individual. The concerns raised about these modes of identification and representation center upon the immediacy with which they may be used to draw conclusions about individuals and their activities, as well as the likelihood that they will be taken as definitively 'true'. These concerns stand in contrast to earlier debates about privacy and information technologies. In the furor over very large databases, the object of concern was *attributes* disclosing the purported *characteristics* of individuals, and in GIS and geo-demographic analysis, the central concern about privacy was focused upon the *inference* of *characteristics* to individuals

based on their location. With the geoweb, identity is disclosed at many fewer levels of abstraction – the digital person no longer needs to be reconstituted from an assemblage of characteristics, but is rather reproduced digitally as their virtual self, in the form of their visual likeness in a place at a certain moment in time, or in terms of their trackable real-time movements in space. There concern is no longer that things about individuals may be revealed, but rather that individuals – as their virtual selves – are disclosed, identifiable, and monitorable *in space*.

4.2. New roles and relationships for privacy actors

The furor over Street View, and Twitter's attempt to preempt similar concerns over GeoAPI, signal profound changes to the roles and relationships of corporate, state, and civil actors in the negotiation of privacy. In the discourses of privacy being advanced by these actors, and the interventions they advance and promote, the social contract around privacy as pertains to geographic information is being remade.

An important element of these transformations is the phenomenon of user-generated content, a core element of the geoweb. In this context, individuals are no longer only or primarily the subjects or claimants of privacy invasion, as they have been in earlier regimes of information provision, but rather are also information producers. As such, civil actors may play a constitutive role in altering their own privacy, the privacy of others, and even the very nature of the social contract around privacy. Take, for example, the phenomenon of 'oversharing', in which individuals reveal highly intimate personal details online (The Economist, 2010). These information-divulging actions of individuals *in aggregate* compromise the privacy rights of all because they shift the socially-mediated boundary between what is public versus what is private (Kleinman, 2010). Twitter's GeoAPI can be seen as a sort of geographic oversharing, potentially normalizing the distribution of information about one's everyday movements to anyone who wishes to follow them online.

This 'responsibilization' of civil actors in the negotiation of privacy is also advanced through approaches used to engineer consent for gathering and disseminating personal information. Street View presumes that all persons present in an imaging frame are 'fair game', and the onus falls on individuals to opt out by requesting removal. Notably, this action can only be taken if the image has already been publicly distributed and an individual has discovered its presence. In the US, the ruling in *Boring vs. Google* affirms this expectation of civil actors. While stipulations that Google announce image collection to the public (Japan, Canada), or respond to image removal requests within a specified time frame (Canada, UK) are more regulatory than the stance taken by the US courts, they are nonetheless predicated on and affirm the idea that civil actors are responsible for their own privacy.

In the geoweb, corporate actors play a different role with respect to information and, thus, the constitution of privacy, than they do with digital information practices that have been at the center of prior debates about privacy. In the case of geo-demographic analysis or credit ratings, corporate actors profit from their own direct analysis and use of information, or from the sale of data or analysis to paying clients. In the geoweb, corporate actors such as Google profit from advertising that accompanies the information and information services they make available, and as such, the clients to whom they are primarily responsible are the purchasers of advertisements. The users of information or information services are secondary.

Secondary uses and users of information have proved difficult for geoweb service providers to anticipate, monitor, regulate, or even know about, and struggles over these uses and users are thrusting these corporate actors into new roles in negotiating privacy. In the case of Twitter, anyone with Internet access can cache geo-tagged tweets and use this information to his or her own ends. This secondary use may violate the information producer's privacy in any number of ways, but it is impossible for Twitter to be aware of, let alone prevent. Solutions that emphasize the mechanics of information storage or dissemination, such as Twitter's time-sensitive data handling, are not sufficient to grapple with these new relationships because 'third parties' are outside the control of the data provider. In grappling with the challenges of these secondary use relationships, some geoweb providers are taking on new responsibilities. In response to malicious secondary uses of Street View imagery in Japan, Google established a formal system for handling such problems. If the third party refuses to remove offensive or identifying imagery that originated from Street View, Google Japan has stated that it will sue the second-party host directly (Zafra 2009). Here, Google takes on the role of the plaintiff and assumes a quasi-regulatory role in information dissemination and use that has been heretofore the domain of the state.

These different responses of Google vis-à-vis privacy concerns raised in Japan and the US further illustrate the contradictory roles of corporate actors in constituting privacy through the geoweb. At the simplest level, Google stands to be a plaintiff in Japan and was a defendant in the US in *Boring vs. Google*. Yet the contradictions are more profound. Providers of geoweb services have invested in the very technologies that others are using for privacy-altering practices, and as such, have a clear motivation to defend against charges of privacy harm, in an effort to ensure that these platforms remain in use. For example, Google itself is partly responsible for the popular dissemination of high-resolution satellite imagery (via its Earth and Maps platoforms) that it then cited in *Boring vs. Google* as part of its defense that in today's technology-laden world, "... complete privacy does not exist" (Google, from its US District Court motion for dismissal of *Boring vs. Google*, available in The Smoking Gun, 2008b, np.). This tautological stance justifies an 'inevitable' loss of privacy based on the presence of imaging technologies that are central to Google's own services (and, is interestingly contradictory to the company's stance in Japan with respect to pursuing malicious secondary data users).[8]

Finally, with respect to the shifting role of state actors, other research suggests that the geoweb is associated with a decline in the presence of national states as information providers (Goodchild, 2007; Haklay et al., 2008) and rising presence of the private sector in this role (Leszczynski, 2010). It is impossible to generalize about what this shift means for states' efforts to negotiate privacy, given the demonstrable diversity of national state responses to geoweb services like Street View. Yet multiple and transformed roles are emerging. In some case, state actors act as mediators or regulators of privacy practices around the geoweb, and in others, as petitioners or plaintiffs. We see the latter in cases where national states have made information modification requests of Google's geoweb services, as in the Japanese and Swiss governments' requests for re-scanning Street View imagery at a lowered camera height, or requests from US, India, China, Pakistan, and South Korea to blur or coarsen the resolution of Google's satellite imagery around military sites.

But as states mandate or petition for various accommodations around privacy around the geoweb, the response of corporate actors clearly varies greatly, as evident in the different accommodations, refusals, and privacy practices that have emerged from governmental requests around Street View imagery. On one hand, we can look to different institutional and state structures to explain this variability. Canada, Switzerland, the UK, and Greece,

[8] Scholars such as Wood et al. (2007) and Lyon (2003) have traced longstanding Anglo-American discourses that reify such losses of privacy as the inevitable outcomes of autonomous technological change.

for example, all have designated branches of the state charged with the protection of privacy, and their mandate extends to the prevention of privacy harms in data capture, retention, or disclosure. In the case of the United States, no similar authority exists and privacy is mediated through the courts, by way of civil actors' claims of privacy harm or loss.

There is clearly much more to learn about how and why these encounters between corporate and state-based regimes of geographic information governance play out differently. Why for instance, has Google blurred imagery at military and other installations deemed sensitive by the US, India, China, and Pakistan, but ignored similar requests made by South Korea (Blamont, 2008; Crampton, 2008; Nourbakhsh et al., 2006; Zook and Graham, 2007)? With respect to privacy accommodations around Street View, why did the company re-image Japan but not Switzerland? Google's explanation references the built environment, noting that because 'streets are narrow', it was necessary to re-image Japan as a matter of information quality (Kirk, 2009). Yet arguably this decision could be motivated by the desire to maintain a significant presence in a country where the population (and potential market base) is far larger than Switzerland, and where Google is fiercely competing with rival Yahoo (Tabuchi, 2009). Varying responses to efforts to regulate Street View around the world further speak to the arbitrary nature of corporate regimes of spatial data governance that, because they are not contained within the boundaries of any one nation-state or institutional jurisdiction, are not definitively accountable to their consumers nor to the governments of countries within which they operate (Leszczynksi, 2010). Our evidence does not enable us to tease out the interplay of corporate profit motives, vernacular landscapes, and cultural variation in social contracts around privacy and the role of the state. But two things are clear: a fuller political economic analysis of the geoweb is needed (Leszczynski 2010); and the balance of powers between the various state and corporate actors in the privacy apparatus is shifting.

Here, we have examined the traces left by struggles over privacy as they are articulated around a particular set of socio-technological practices – the geoweb. Examining these negotiations illuminates shifts in civil, institutional, and corporate understandings of 'privacy' around geospatial technologies, as well as to altered expectations of the *kinds* of things that are considered private and where and when we may anticipate that our privacy is 'protected.' All of this – from discourses both public and corporate, to the approaches for its protection – constitutes a fundamental change in the meanings and practices of privacy.

5. Conclusion

In the age of Web 2.0, privacy has gone spatial. New modes of collecting, representing, and disseminating spatial information are at the center of contemporary societal struggles over privacy. Geoweb services have sparked heated struggles in mainstream and citizen media, courts, and legislative bodies over actual and anticipated privacy harms. These public struggles transform privacy. They constitute and reconstitute privacy through their articulation of actual and anticipated harms, proposed and implemented remedies for these supposed harms, and resistance or acquiescence to the assertions advanced by other actors around these things. In the process, we also see a reworking of the roles and responsibilities of key players in the privacy apparatus.

The furor over Street View and Twitter's GeoAPI also more clearly define some of what is 'new' with respect to the representational practices of the geoweb, as compared to prior spatial information technologies. Specifically, geo-tagged images and snippets of self-authored text reveal the supposed presence of individual bodies or objects, rather than only their attributes. Further, identification and disclosure are more immediate, and less abstracted than in, say, a numerical database. In the case of digital images, whatever is revealed is underwritten by the primacy or 'truth power' afforded to visual artifacts.

More broadly, a shift in the nature and scale of privacy as a social relation is underway. In prior accounts, the notion of privacy as a social contract has often referenced implied understanding between subjects (be they consumers or citizens) and a secondary party (the state or corporation) who cede a certain degree of autonomy or give up certain freedoms in exchange for the right to privacy, which the second party is expected to ensure and enforce (Allen, 1987). Ensuring the privacy rights of individuals increasingly involves negotiating shifts in the meaning and constitution of privacy that are located beyond the person, as well as beyond simple first party/second party relationships. The challenges presented by secondary data users or national government requests to blur state secrets, among other developments, attest to the need to negotiate new dimensions of 'privacy' that are constituted through the geoweb and its attendant practices.

Against this backdrop, it is clear that we need new modes of theorizing geographic information technologies that allow us to begin to grapple with, rather than elide, what is 'new' about new spatial media. We have begun to show here how the geoweb introduces new data primitives that emphasize new forms of, and metaphors for, representation that exceed extant categories and frameworks. For example, the geoweb forces us to think beyond a singular technology (GIS) and its primary representational output, the map, even while socio-political research on the geoweb is bound to be informed to some degree by propositions emerging from critical GIS research.

Struggles over the geoweb are implicated in a much broader public debate over the social, political and technical transformation of privacy in a Web 2.0 world. The demonstrably spatial dimensions of privacy bring to the fore new considerations that must be taken into account as privacy's desirability and sustainability are being publically negotiated. Actors with a vested interest in circumventing existing privacy protections may claim that there is no such thing as privacy in an age of freely available high-resolution satellite imagery (as in *Boring vs. Google*), suggest that privacy should just be 'done away with' to eliminate obstacles to efficiency (as per *Wired*), or suggest that Web 2.0 practices such as blogging and social networking normalize an erosion of privacy among the next generation (West, 2009). Yet the cases we have explored here suggest that privacy – despite being actively renegotiated – remains highly contested. These contestations matter because they have consequences for how we interact with others, and the kinds of protections we expect and interventions we allow, with overlapping and competing stakes for the actors involved.

Acknowledgements

We are grateful for the helpful suggestions of the editor and three anonymous reviewers. The research was supported under National Science Foundation grant BCS-0849625.

References

Aday, S., Livingston, S., 2009. NGOs as intelligence agencies: The empowerment of transnational advocacy networks and the media by commercial remote sensing in the case of the Iranian nuclear remote program. Geoforum 40 (4), 514–522.

Allen, A.L., 1987. Taking Liberties: Privacy, Private Choice, and Social Contract Theory. University of Cincinnati Law Review 56 (1–2).

BBC News, 2010a. Australia orders Google 'privacy breach' investigation. BBC. <http://news.bbc.co.uk/2/hi/world/asia_pacific/10249091.stm>.

BBC News, 2010b. Google accused of criminal intent over StreetView data. BBC. <http://news.bbc.co.uk/2/hi/technology/10278068.stm>.

BBC News, 2010c. Google's Street View faces multi-state US probe. BBC. <http://news.bbc.co.uk/2/hi/technology/10375623.stm>.
BBC News, 2009. Switzerland takes Google to court. BBC. <http://news.bbc.co.uk/2/hi/business/8358908.stm>.
Bishr, M., Mantelas, L., 2003. A trust and reputation model for filtering and classification of knowledge about urban growth. GeoJournal 72 (2/3), 229–237.
Blamont, J., 2008. We the people: Consequences of the revolution in the management of space applications. Space Policy 24 (1), 13–21.
Blumberg, A. J., Eckersley, P., 2009. On locational privacy, and how to avoid losing it forever?. Electronic Frontier Foundation. <http://www.eff.org/wp/locational-privacy>.
Bradley, T., 2009. Google Street View Battle Highlights Privacy Challenge. San Francisco Chronicle. <http://www.sfgate.com/cgibin/article.cgi?f=/g/a/2009/11/16/urnidgns002570F3005978D80025766E005191D6.DTL>.
Capper, S., 2009. Google faces court action over Street View. swissinfo.ch. <http://www.swissinfo.ch/eng/front/Google_faces_court_action_over_Street_View.html?siteSect=105&sid=11489632&ty=st>.
CNN. 2009. Google Street View blacked out in Greece. CNN.com/europe. <http://edition.cnn.com/2009/WORLD/europe/05/13/greece.google.street.view.blocked/index.html#cnnSTCText>.
Cohen, N., 2009. Refining the Twitter Explosion. The New York Times. <http://www.nytimes.com/2009/11/09/business/09link.html>.
Crampton, J.W., 2009a. Being Ontological. Environment and Planning D: Society and Space 27 (4), 603–608.
Crampton, J.W., 2009b. Cartography: maps 2.0. Progress in Human Geography 33, 91–100.
Crampton, J., 2008. Mapping without a net: neogeography in the 21st Century. Virtual Seminars in GI Science and Technology: Joint Worldwide Universities Network, RGS (with IBG) Quantitative Methods Research Group and UCGIS. Online, virtual seminar.
Crampton, J., 1995. The ethics of GIS. Cartography and Geographic Information Systems 22 (1), 84–89.
Crang, M., 2003. The hair in the gate: visuality and geographical knowledge. Antipode 35 (2), 238–243.
Cross, M., 2009. Michael Cross: The information commissioner was right to defend Google Street View. The Guardian. <http://www.guardian.co.uk/commentisfree/libertycentral/2009/apr/26/google-street-view-privacy>.
Crowe, J., 2009. Twitter Supports Geotagging. The Map Room. <http://www.mcwetboy.net/maproom/2009/11/twitter_support.php>.
Curry, M., 1998. Digital Places: Living With Geographic Information Technologies. Routledge, London.
Curry, M., 1995a. Rethinking rights and responsibilities in geographic information systems: beyond the power of the image. Cartography and Geographic Information Systems 22 (1), 58–69.
Curry, M., 1995b. GIS and the inevitability of ethical inconsistency. In: Pickles, J. (Ed.), Ground Truth: The Social Implications of Geographic Information Systems. Guilford, London, pp. 68–87.
Daston, L., Galison, P., 2007. Objectivity. Zone Books, New York.
Dave, B., 2007. Space, sociality, and pervasive computing. Environment and Planning B: Planning and Design 34 (3), 381–382.
Dodge, M., Kitchin, R., 2007. Outlines of a world coming into existence': pervasive computing and the ethics of forgetting. Environment and Planning B: Planning and Design 34 (3), 431–445.
Dodge, M., Perkins, C., 2009. The 'view from nowhere'? Spatial politics and cultural significance of high-resolution satellite imagery. Geoforum 40 (4), 497–501.
The Economist, 2010. Location-based services on mobile phones: Follow me. The Economist. <http://www.economist.com/businessfinance/displaystory.cfm?story_id= 15612291>.
Elwood, S., 2010. Geographic information science: Emerging research on the societal implications of the geoweb. Progress in Human Geography 34 (3), 349–357.
Elwood, S., 2009. Geographic information science. New geovisualization technologies–emerging questions and linkages with GIScience research. Progress in Human Geography 33 (2), 256–263.
Electronic Frontier Foundation, 2009. EFF and ACLU Urge Court to Reject Warrantless GPS Tracking. Electronic Frontier Foundation. <http://www.eff.org/press/archives/2009/03/03-0>.
Fee, J., 2009. Twitter Acquires GeoAPI; The New GeoLocation Platform of Choice? James Fee GIS Blog. <http://www.spatiallyadjusted.com/2009/12/23/twitter-acquires-geoapi-the-new-geolocation-platform-of-choice/>.
Flanagin, A.J., Metzger, M.J., 2008. The credibility of volunteered geographic information. GeoJournal 72 (3–4), 137–148.
Frank, 2009. Cops Can't Track Cars with GPS Without Warrant. VerySpatial.com. <http://veryspatial.com/2009/10/cops-cant-track-car-with-gps-without-warrent/>.
Graham, S., 2005. Software-sorted geographies. Progress in Human Geography 29 (5), 562–580.
Graham, S., 1999. Spaces of surveillant simulation: new technologies, digital representations, and material geographies. Journal of Planning Literature 14 (1), 483.
Graham, S., Wood, D., 2003. Digitizing surveillance. Categorization, space, inequality. Critical Social Policy 23 (2), 227–248.
Graham, S., 2002. CCTV: the stealthy emergence of a fifth utility? Planning Theory and Practice 3 (2), 237–241.
Goodchild, M., 2007. Citizens as sensors: the world of volunteered geography. GeoJournal 69 (4), 211–221.
Goodin, D., 2009. US court urged to block warrantless GPS tracking. The Register. <http://www.theregister.co.uk/2009/03/04/warrantless_gps_tracking/>.
Goss, J., 1995a. Marketing the new marketing: the strategic discourse of geodemographic information systems. In: Pickles, J. (Ed.), Ground Truth: The Social Implications of Geographic Information Systems. Guilford, London, pp. 130–170.
Goss, J., 1995b. We know who you are and we know where you live: The instrumental rationality of geodemographic systems. Economic Geography 7 (1), 171–198.
Haklay, M., Singleton, A., Parker, C., 2008. Web mapping 2.0: the Neogeography of the geoweb. Geography Compass 2 (6), 2011–2039.
Harris, C., 2006. The omniscent eye: satellite imagery, battleship awareness, and thestructures of the imperial gaze. Surveillance and Society 4 (1–2), 101–122.
Harris, T., Weiner, D., 1996. GIS and society: The social implications of how people, space, and environment are represented in GIS, Scientific report for NCGIA Initiative 19 Specialist Meeting. NCGIA Technical Report 96-7. <http://www.ncgia.ucsb.edu/Publications/Tech_Reports/96/96-7.PDF>.
Haines, L., 2009a. Greece grounds Google's Street View fleet. The Register. <http://www.theregister.co.uk/2009/05/12/street_view_greece/>.
Haines, L., 2009b. Street View in (kind of) Swiss roll-over. The Register. <http://www.theregister.co.uk/2009/10/15/street_view_switzerland/>.
Hyde, A., 2010. Committing Location Based Service Suicide. Andrew Hyde. <http://andrewhy.de/committing-location-based-service-suicide/>.
Kingsbury, P., Jones, J.P., 2009. Walter Benjamin's Dionysian adventures on Google Earth. Geoforum 40 (4), 502–513.
Kirk, J., 2009. Swiss Contend Google Doesn't Blur Street View Enough. PC World. <http://www.pcworld.com/article/182150/swiss_contend_google_doesnt_blur_street_view_enough.html>.
Kiss, J,. 2009. Google wins Street View privacy case. The Guardian. <http://www.guardian.co.uk/media/2009/feb/19/google-wins-street-view-privacy-case>.
Klapper, B. S., 2009. Swiss official tells Google to erase street views. Breitbart. <http://www.breitbart.com/article.php?id=D9A9C8QO1&show_article=1>.
Kleinman, Z., 2010. How online life distorts privacy rights for all. BBC. <http://news.bbc.co.uk/2/hi/technology/8446649.stm>.
Krikonian, R., 2009. Twitter API Wiki / Geotagging API Best Practices. Twitter. <http://apiwiki.twitter.com/Geotagging-API-Best-Practices>.
Koerner, B. I., 2009. Jamie Heywood – Forget Medical Privacy. Wired. <http://www.wired.com/techbiz/people/magazine/17-10/ff_smartlist_heywood>.
Leszczynski, L., 2009. Poststructuralism and GIS: Is there a 'disconnect'? Environment and Planning D: Society and Space 27 (4), 581–602.
Leszczynski, A., 2010. Situating Neogeograpy in Political Economy. Paper presented at the Association of American Geographers Annual Conference, Washington, DC, 14-18 April.
Letham, G., 2009. Twitter Scoops up Mixer Labs, creators of the Geo API. AnyGeo. <http://blog.gisuser.com/?p=5750>.
Lyon, D., 2003. Introduction. In: Lyon, D. (Ed.), Surveillance as Social Sorting: Privacy, risk and digital discrimination. Routledge, London and New York.
Madden, L., 2009. Do You Care About Privacy? Augmented Planet. <http://www.augmentedplanet.com/2009/11/do-you-care-about-privacy/>.
Meller, P., 2008. EU Raises Privacy Issue for Google Street View. PC World. <http://www.pcworld.com/businesscenter/article/145927/eu_raises_privacy_issue_for_google_street_view.html?tk=rel_news>.
Mummidi, L., Krumm, J., 2008. Discovering points of interest from users' map annotations. GeoJournal 72 (3–4), 215–227.
Norris, C., 2003. From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In: Lyon, D. (Ed.), Surveillance as Social Sorting: Privacy, risk and digital discrimination. Routledge, London and New York.
Nourbakhsh, I., Sargent, R., Wright, A., Cramer, K., McClendon, B., Jones, M., 2006. Mapping disaster zones. Nature 439 (7078), 787–788.
O'Reilly T., 2005. What is Web 2.0. The O'Reilly Network. <http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html>.
out-law.com, 2009. Google to delete Street View source images. The Register. <http://www.theregister.co.uk/2009/06/16/google_street_view_source_deletion/>.
Parks, L., 2009. Digging into Google Earth: An analysis of "Crisis in Darfur". Geoforum 40 (4), 535–545.
Paul, I., 2009a. Google Street Views Faces Privacy Critics in Japan and Greece. Today @ PC World. <http://www.pcworld.com/article/164810/google_street_views_faces_privacy_critics_in_japan_and_greece.html>.
Paul, I., 2009b. Twitter Geotagging: What You Need to Know. Today @ PC World. <http://www.pcworld.com/article/182729/twitter_geotagging_what_you_need_to_know.html>.
Perez, J. C., 2009. Judge Dismisses Google Street View Case. PC World. <http://www.pcworld.com/article/159740/judge_dismisses_google_street_view_case.html?tk=rel_news>.
Perkins, C., Dodge, M., 2009. Satellite imagery and the spectacle of secret spaces. Geoforum 40 (4), 546–560.
Phillips, D., Curry, M., 2003. Privacy and the phenetic urge: Geodemographics and the changing spatiality of local practice. In: Lyon, D. (Ed.), Surveillance as Social Sorting: Privacy, risk and digital discrimination. Routledge, London and New York.
Pickles, J., 1995. Representations in an electronic age: Geography, GIS, and democracy. In: Pickles, J. (Ed.), Ground Truth: The Social Implications of Geographic Information Systems. Guilford, New York, pp. 1–30.
Pickles, J., 1991. Geography, GIS, and the surveillant society. Papers and Proceedings of Applied Geography Conferences 14, 80–91.

Pleace, N., 2007. Workless people and surveillant mashups: Social policy and data sharing in the UK. Information. Communication & Society 10 (6), 943–960.
Pomfret, K., 2010. Google Street View: Are We Looking At It The Right Way? Spatial Law and Policy. <http://spatiallaw.blogspot.com/2010/06/google-street-view-are-we-looking-at-it.html>.
Raphael, J. P., 2009. Google Declares: 'Complete Privacy Does Not Exist'. Today @ PC World. <http://blogs.pcworld.com/staffblog/archives/007374.html?tk=rel_news>.
Reuters, 2010. US court orders Google to copy data in Wi–Fi case. Reuters. <http://www.reuters.com/article/idUSN2713025120100527>.
Rodrigues, J., 2009. Google Street View's headaches around the world. The Guardian. <http://www.guardian.co.uk/technology/2009/nov/29/google-street-view>.
Rose, G., 2007. Visual Methodologies: An Introduction to the Interpretation of Visual Materials. (2nd ed.). Sage, London.
Rose-Redwood, R., 2006. Governmentality, geography, and the geo-coded world. Progress in Human Geography 30 (4), 469–486.
Ryan, J.R., 2003. Who's Afraid of Visual Culture. Antipode 35 (3), 232–237.
Sarver, R,. 2009. Think Globally, Tweet Locally. Twitter Blog. <http://blog.twitter.com/2009/11/think-globally-tweet-locally.html>.
Scarcella, M., 2009. D.C. Circuit Examines Warrantless GPS Surveillance. The BLT: The Blog of Legal Times. < http://legaltimes.typepad.com/blt/2009/11/dc-circuit-examines-warrantless-gps-surveillance.html>.
Scharl, A., Tochtermann, K., 2007. The geospatial web: how geobrowsers, social software and the Web 2.0 are shaping the network society. Springer, London.
Schmidt, S., 2009a. Privacy not protected on Google Street View, MPs told. National Post. <http://www.nationalpost.com/news/story.html?id=2133506>.
Schmidt, S., 2009b. Google Street View not doing enough to protect Canadians' privacy, MPs told. Ottawa Citizen. <http://www.ottawacitizen.com/Google+Street+View+doing+enough+protect+Canadians+privacy+told/2133497/story.html>.
Schutzberg, A., 2009. The Value of Location-based Tweets. All Points Blog. <http://apb.directionsmag.com/archives/6798-The-Value-of-Location-based-Tweets.html>.
Shankland, S., 2008. Google begins blurring faces in Street View. CNet News. <http://news.cnet.com/8301-10784_3-9943140-7.html>.
Sheppard, E., 1995. GIS and society: Towards a research agenda. Cartography and Geographic Information Systems 22 (1), 5–16.
Shiels, M., 2010a. Google admits Wi–Fi data collection blunder. BBC. <http://news.bbc.co.uk/2/hi/technology/8684110.stm>.
Shiels, M., 2010b. US tech coalition calls for new online privacy laws. BBC. <http://news.bbc.co.uk/2/hi/technology/8595775.stm>.
Siddique, H., 2009. Greece's dim view of Street View. The Guardian. <http://www.guardian.co.uk/technology/2009/may/12/google-street-view-greece-privacy>.
Smith, H., 2009. Google Street View cars banned from Greece. The Guardian. <http://www.guardian.co.uk/technology/2009/may/12/google-street-view-banned-greece>.
The Smoking Gun, 2008a. Couple Sues Google Over "Street View". The Smoking Gun. <http://www.thesmokinggun.com/archive/years/2008/0404081google1.html>.
The Smoking Gun, 2008b. Google: "Complete Privacy Does Not Exist". The Smoking Gun. <http://www.thesmokinggun.com/archive/years/2008/0730081google1.html>.
Solove, D., 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review 154 (3), 477–560.
Sui, D.Z., 2000. Visuality, Aurality, and Shifting Metaphors of Geographical Thought in the Late Twentieth Century. Annals of the Association of American Geographers 90 (2), 322–343.
Tabuchi, H., 2009. In Japan, an Odd Perch for Google: Looking Up at the Leader. The New York Times. <http://www.nytimes.com/2009/11/30/technology/internet/30google.html>.
Trapani, G., 2009. Details on Twitter's Imminent Geolocation Launch. Smartware. <http://smarterware.org/3419/details-on-twitters-imminent-geolocation-support-launch>.
Tuan, Y.-F., 1979. Sight and Pictures. Geographical Review 69 (4), 413–422.
Tulloch, D.D., 2008. Is VGI Participation? From vernal pools to video games. GeoJournal 72 (3–4), 161–171.
Turner, A., 2006. Introduction to Neogeography. O'Reilly, Sebastopol, CA.
Uprichard, E., Burrows, R., Parker, S., 2009. Geodemographic code and the production of space. Environment and Planning A 41 (12), 2823–2835.
Weaver, M. 2009. Google Street View cleared of breaking Data Protection Act. The Guardian. <http://www.guardian.co.uk/technology/2009/apr/23/google-street-view-data-protection-cleared>.
West, H., 2009. Is Online Privacy a Generational Issue? Pew Internet & American Life Project. <http://www.pewinternet.org/Media-Mentions/2009/Is-Online-Privacy-a-Generational-Issue.aspx>.
White, A., 2009. Google warned by EU over Street View map photos. Yahoo! News. <http://news.yahoo.com/s/ap/20100226/ap_on_hi_te/eu_eu_google_data_privacy>.
Williams, J., 2009. Google Japan fights concerns about Street View. Examiner.com. <http://www.examiner.com/x-16352-Japan-Headlines-Examiner~y2009m9d4-Google-Japan-fights-concerns-about-Street-View>.
Wong, T. S. K., 2009. Google Street View a privacy worry. The Toronto Star. <http://www.thestar.com/special/article/713806–google-street-view-a-privacy-worry>.
Wood, D.M., Lyon, D., Abe, K., 2007. Surveillance in Urban Japan: A Critical Introduction. Urban Studies 44 (3), 551–568.
Zafra, A., 2009. Google Street View in Japan Faces Various Complaints. Search Engine Journal. <http://www.searchenginejournal.com/google-street-view-in-japan-faces-various-complaints/13048/>.
Zook, M., Graham, M., 2007. The creative reconstruction of the Internet: Google and the privatization of cyberspace and DigiPlace. Geoforum 38 (6), 1322–1343.