

UC Santa Barbara

UC Santa Barbara Previously Published Works

Title

Please Enter Your Home Location: Geoprivacy Attitudes and Personal Location Masking Strategies of Internet Users

Permalink

<https://escholarship.org/uc/item/2tk78817>

Journal

Annals of the American Association of Geographers, 110(3)

ISSN

2469-4452

Authors

Seidl, Dara E
Jankowski, Piotr
Clarke, Keith C
[et al.](#)

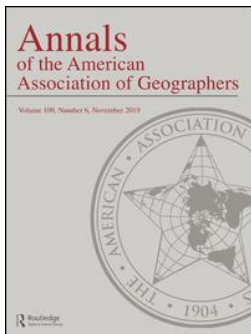
Publication Date

2020-05-03

DOI

10.1080/24694452.2019.1654843

Peer reviewed




Please Enter Your Home Location: Geoprivacy Attitudes and Personal Location Masking Strategies of Internet Users

Dara E. Seidl, Piotr Jankowski, Keith C. Clarke & Atsushi Nara

To cite this article: Dara E. Seidl, Piotr Jankowski, Keith C. Clarke & Atsushi Nara (2019): Please Enter Your Home Location: Geoprivacy Attitudes and Personal Location Masking Strategies of Internet Users, *Annals of the American Association of Geographers*, DOI: 10.1080/24694452.2019.1654843


To link to this article: <https://doi.org/10.1080/24694452.2019.1654843>

 View supplementary material 

 Published online: 10 Oct 2019.

 Submit your article to this journal 

 Article views: 43

 View related articles 

 View Crossmark data 

Please Enter Your Home Location: Geoprivacy Attitudes and Personal Location Masking Strategies of Internet Users

Dara E. Seidl,^{*,†} Piotr Jankowski,^{*,‡} Keith C. Clarke,[†] and Atsushi Nara^{*}

^{*}Department of Geography, San Diego State University

[†]Department of Geography, University of California, Santa Barbara

[‡]Institute of Geoecology and Geoinformation, Adam Mickiewicz University

Location masking, or geomasking, is a practice typically undertaken by data stewards who wish to release a georeferenced data set without infringing on the privacy of those whose data are involved. With numerous opportunities to transmit our personal locations through electronic devices, individuals have the agency through masking to stem the flow of their location data or otherwise engage in obscuring their locations. Relatively little is known about the factors that influence individuals to protect their location privacy and the extent to which they do so. Joining a growing recognition of individual-level privacy efforts, this study examines the predictors of personal-level location masking and the relationships among geoprivacy-related knowledge, attitudes, and behavior. Using a probability-based sample and an open online sample from California, this study finds that in situ personal masking behavior is consistent across demographic groups. A key attitude influencing whether or not participants choose to mask location is trust in Web sites to protect their personal data. Greater knowledge about how location data are transmitted and higher concern for privacy are positively correlated with masking behavior. *Key Words:* geomasking, geoprivacy, obfuscation, privacy, survey.

地点屏蔽，或是地理屏蔽，是数据管理专员为了释放标示地理的数聚集、但不侵犯数据所有者的隐私时所采用的特定方法。通过电子设备传输我们的个人地点的机会众多，个人具有通过屏蔽来阻止其地点数据的流动抑或是反之从事混淆其地点的能动性。影响个人保护其地点隐私、以及他们这样做的程度之因素却相对不为人知。本研究接合对个人层级隐私之努力逐渐增加的认识，检视个人层级地点屏蔽的预测因素，以及与地理隐私相关的知识、态度与行为之间的关系。本研究运用来自加州的一个根据或然率的样本以及开放式网路样本，发现原地的个人屏蔽行为在各人口群体之间是一致的。影响参与者是否选择屏蔽地点的主要态度，是信任网站保护其个人数据。对于地点数据如何传递有较多的知识，以及对隐私的较高考量，则与屏蔽行为呈现正相关。关键词：地理蒙蔽，地理隐私，使困惑，隐私，调查。

El ocultamiento de la localización, o geoenmascaramiento, es una práctica que típicamente usan los administradores de datos que quieren liberar un conjunto de datos georreferenciados sin vulnerar la privacidad de aquellos cuya información está involucrada. Con las numerosas opciones disponibles para transmitir nuestras localizaciones personales a través de aparatos electrónicos, la gente puede ejercer agencia por medio del ocultamiento para contener el flujo de sus datos de localización, o, de otro modo, puede actuar para oscurecer sus ubicaciones. Relativamente poco se conoce acerca de los factores que influyen sobre los individuos en términos de proteger su privacidad locacional, y sobre el alcance con el que ellos lo hacen. Uniéndonos al creciente reconocimiento de los esfuerzos por asegurar la privacidad individual, este estudio examina los predictores del ocultamiento de localización a nivel personal y las relaciones entre el conocimiento asociado con geoprivacidad, las actitudes y el comportamiento. Usando una muestra basada en probabilidad y una muestra abierta online en California, este estudio encuentra que el comportamiento de ocultamiento personal in situ es consistente a través de los grupos demográficos. Una actitud clave que determina si los participantes deciden o no enmascarar la localización es el confiar en la protección de sus datos personales en sitios Web. Un conocimiento más grande sobre el modo como los datos de localización se transmiten y una mayor preocupación por la privacidad se correlacionan positivamente con la conducta del ocultamiento. *Palabras clave:* geoenmascaramiento, geoprivacidad, ofuscación, privacidad, sondeo.

Location data permeate our frequently used digital services and are routinely bought and sold by private entities. Geographic data are collected when we swipe credit cards, browse the Internet, post on social media, and use location-based services (LBS). Such data collection and

subsequent transmission to third parties often occur without the knowledge or consent of the data subject. This practice is in direct opposition to the concept of location privacy, or *geoprivacy*, which refers to the right of individuals to control when and how their personal location data are shared (Duckham and Kulik 2006). Efforts to protect geoprivacy in geographic research have primarily involved geomasking techniques, which introduce deliberate inaccuracy into geographic data to protect both confidentiality and spatial distribution (Armstrong, Rushton, and Zimmerman 1999). Applications of geomasking are intended for releases of geographic data and suggest a structure in which trusted experts make decisions on the appropriate parameters to protect the privacy of individual data subjects. In this study, we examine the reverse of this structure: a bottom-up evaluation of the choices that individuals make to obscure, or mask, their own locations. We refer to the practice of obscuring one's own location data as *personal location masking*. In studying personal location masking, we deployed an online survey to answer two principal questions:

1. In what ways do adults attempt to mask their location data?
2. How do geoprivacy knowledge and attitudes influence these personal location masking behaviors?

Geoprivacy-related attitudes and behaviors merit study not only because the traditional notion of geoprivacy is eroding under pervasive data collection but because this erosion leads to personal harm. Despite the refrain that privacy is nothing to worry about for those who have “nothing to hide” (Solove 2007), localized individual harms from unwanted location disclosure rise with increased data collection. In 2016, a California man was sentenced to prison for using geotagged Instagram photos to locate and burglarize thirty-three women (Puente 2016). Undesired location tracking is often applied in domestic abuse cases, where abusers install spyware on victims' smartphones or hide Global Positioning System (GPS) trackers in shoes or cars (Shahani 2014). Surreptitious location collection is also playing out on a larger scale. In November 2017, reports emerged that Google collected cell tower locations when Android consumers had location services turned off, to within a quarter-mile of accuracy (Liao 2017). Furthermore, the conversion of location data to a commodity can cost consumers who do not share it. For example, the insurance practice of

offering lower rates to drivers who install vehicle GPS devices not only leads to disparate costs of driving depending on the neighborhood of commute (Scism 2016) but penalizes customers who decline to share their location (Keßler and McKenzie 2018).

Calls for protecting geoprivacy are not new. Mid-1990s research discusses the growing threat to privacy from geodemographics and large databases (Goss 1995; Curry 1997). The geographic information systems (GIS) and society debates over privacy revived terms such as the *panopticon*, a symbol of total surveillance and control (Dobson and Fisher 2007), and introduced *geoslavery*, where an entity exerts control over the location of an individual (Dobson and Fisher 2003). Today, privacy concerns are growing. The 2014 President's Council of Advisors on Science and Technology issued an influential report on big data, citing location privacy as one of the predominant issues in a data-driven world (Council of Advisors on Science and Technology [PCAST] 2014). In 2016, the National Science and Technology Council (NSTC) released a National Privacy Research Strategy, establishing goals for federal investment, among which is measuring privacy desires and impacts (NSTC 2016). This study is a step toward that goal. The work is also relevant in the wake of the European Union (EU 2016) General Data Protection Regulation (GDPR), which became enforceable in May 2018. The GDPR restricts how companies collect and share personal records, levying fines for privacy violations.

The following sections discuss the history of geomasking, location collection mechanisms, theoretical underpinnings, strategies and motivations for personal location masking, and related survey research. This is followed by a discussion of the study conceptualization and variables hypothesized to influence personal location masking behavior. The Methods section reviews the sampling and questionnaire design, as well as the selected procedures for survey analysis. In the Results, we present the correlates of personal location masking, as well as its predictors in ordinal logistic regression, concluding with a discussion of the study implications.

Geomasking Techniques

An active body of research within the realm of geoprivacy involves geomasking techniques. These techniques displace geographic data to protect spatial

distribution and the privacy of data subjects (Armstrong, Rushton, and Zimmerman 1999). Masking techniques include random and weighted random perturbation (Kwan, Casas, and Schmitz 2004), donut masking (Hampton et al. 2010), Gaussian perturbation (Zandbergen 2014), affine transformations (Armstrong, Rushton, and Zimmerman 1999), grid masking (Seidl, Jankowski, and Tsou 2016), Voronoi masking (Seidl et al. 2015), location swapping (Zhang et al. 2016), and masking based on the Military Grid Reference System (MGRS; Clarke 2015). Similar to geomasking is the computer science approach of *obfuscation*, which refers to a degradation of the quality of spatial data. Obfuscation and the related concept of differential privacy (Dwork 2006) are often studied in the context of smartphones.

As privacy strategies, masking and obfuscation are intended not for the average user but for an expert behind the scenes making decisions on the acceptable degree of location privacy. These techniques have a typical use scenario: Geographic data containing human subjects are set to be released and must be altered to maintain confidentiality. In a world where personal location disclosure does not exist outside of these limited data releases, geomasking would be effective in maintaining confidentiality. Internet users routinely encounter opportunities to reveal their current and future locations, however.

Location Collection Mechanisms

Location data are constantly emitted as a by-product of our daily technological interactions. Location capture mechanisms include GPS, Internet Protocol (IP) address, WiFi access points, cell tower communications, geosocial check-ins, geotagged photos, and semantic content of social media posts. Some of these mechanisms require input from the user (check-ins, volunteered geographic information [VGI]), whereas other forms of location data are passively and, often, furtively collected. For example, there are several ways in which smartphones continue to collect or emit location when location services are turned off. When searching for possible WiFi connections, WiFi-enabled devices release signals, including a media access control (MAC) address, which is a unique and persistent device identifier, and the name of each saved WiFi network to which the device previously established a connection (Kofman 2019). These WiFi probe requests can spell out a thorough location

history, which might include home networks, airports, hotels, and coffee shops visited by a user.

Bluetooth serves as another positioning technology. The proximity marketing industry employs beacons emitting Bluetooth Low Energy (BLE), such as Apple's iBeacon, to microlocate consumers and offer tailored deals when they enter a retail location (Hern 2014). Beacons register when smartphones enter and exit a given location and provide tracking throughout retail stores. Another smartphone technology, near-field communication (NFC), supports mobile payment systems Apple Pay and Google Wallet and enables credit card transactions when phones are within a few centimeters of a reader. Car manufacturers, including Tesla, Audi, Mercedes-Benz, and Hyundai, are increasingly equipping vehicles with smartphone NFC and BLE technology as digital keys (Barry 2018; Swedberg 2019). The adoption of these technologies leads to new and varied recipients of personal location data.

Cell tower communication is also used to capture the locations of smartphone users. In addition to Google's collection of cell tower locations from Android phones (Liao 2017), it was revealed in 2019 that AT&T, T-Mobile, and Sprint were selling real-time cell tower customer locations to bounty hunters and bail bond companies (Cox 2019). Aside from GPS, Bluetooth, NFC, and cell tower triangulation, location can be collected from otherwise unassuming data points. One study demonstrated that applications reading real-time smartphone power consumption levels can successfully convert these data into location information, as power demand increases with distance from a cell phone tower (Michalevsky et al. 2015).

Location data have varying levels of accuracy. For instance, smartphone GPS is typically more accurate than cell tower triangulation and is thus sold at a higher price by telecommunications companies (Cox 2019). IP address geocoding, a process used to geolocate Internet-connected devices by matching their IP addresses to a database, suffers from inconsistent accuracy. Recent reports have documented the fallout from IP address geocoding in lost phone tracking applications. When a GPS position is not found, these applications geocode IP address, and even if the geocoding result is as broad as a city, state, or country, the coordinates of the centroid of these administrative regions are returned. This has led to tense encounters between police, device owners, and unwitting residents who happen to live at these boundary centroids in Kansas (Hill 2016) and South Africa (Hill 2019).

Theoretical Underpinnings

From the myriad mechanisms for location data capture and leakage, it is clear that personal data flows cannot be reduced to a single device, platform, or network. For this reason, Marwick and Boyd (2014) characterized the flow of personal data as belonging to networked information ecologies that tend to capture and recirculate it without the awareness of the original data subject. Other researchers characterize privacy as no longer limited to disclosures of personally identifying information (PII) but as a set of “family resemblances” of persons and information, which includes information collection, processing, dissemination, and invasion (Solove 2007). Nissenbaum (2009) introduced the contextual integrity approach, in which privacy is not the right to control personal information but to have the majority of your societal expectations met with regard to your information flows.

Other privacy experts have attempted to make sense of societal reactions to pervasive location collection. Crawford (2014) described the public affect in the wake of the 2013 Edward Snowden revelations of the scale of surveillance activities by national security agencies as one of surveillant anxiety. Crawford defined this as a fear that the data we shed simultaneously overreveal and misrepresent us. With supporting survey research, Leszczynski (2015) argued that the public affect is better characterized as an “anxiety of control,” meaning that individuals are more concerned with directing their own personal location information flows in the midst of feeling that such efforts might be futile. She argued that individual response to the erosion of privacy is at the origins of devices, applications, and services, rather than with the practices of data capture or use in surveillance. If the societal response to the loss of privacy is an increasing concern with application-level control, it is reasonable that Internet users would attempt to stem their location data flows through personal location masking.

Personal Location Masking

Social media applications, such as Facebook, Twitter, and Instagram, often provide users with some degree of control over the locations posted for others to see, even if the companies themselves collect more precise location data. Users can opt to

mask their locations by turning off location services; using technology to reroute an IP address; providing inaccurate home address information; limiting posts with geographic content, such as check-ins or geo-tagged photos; and otherwise reducing the resolution of any geographic data provided. Swanlund and Schuurman (2016) argued that Tor, an onion routing technology used to alter IP address, is a prime example of resistance to geosurveillance.

Internet users might be more familiar with the online classifieds Web site, Craigslist, as a mechanism for regulating how they share location when posting. When placing an ad, a user can populate the fields for street, cross-street, city, state, and postal code, as well as drag a pin around on the map. Although intended for users to drag the pin to a more exact location, this option could also be used to displace the point to hide the exact location, as with a geographical mask. *Obfuscation*, a recent book by legal privacy experts Brunton and Nissenbaum (2015), provides guidance on data masking strategies at the individual level. As alternatives to encryption and the use of Tor, recommendations include using applications that flood collection technologies with fake, misleading, or ambiguous data to obstruct and evade surveillance. For example, the Firefox extension TrackMeNot, obfuscates actual user Web searches by hiding them in randomized fake search queries. Although multiple technologies exist for Internet users to mask their own locations, the extent to which users employ such strategies is unknown.

Motivations for Personal Location Masking

This study focuses on personal location masking as an act of privacy protection. Alternate considerations, however, can motivate individuals to modify location, one of which is to gain a benefit not otherwise available. For example, some Netflix subscribers alter IP addresses to watch content that is not available in their regions of residence, and some players of Pokémon Go modify GPS locations to acquire more game rewards (Zhao and Chen 2017). The benefits of altering location data can include money, prizes, or status. Some social media users document “fake vacations” to expensive or exotic locales to gain status or invite the envy of others. A company called Fake a Vacation offers customers edited photos of themselves in Hawaii or at the Grand Canyon for a much lower cost than an actual trip. There are

also cases of individuals masking their locations to oppose the surveillance of others, rather than protect their own privacy. In a notable 2009 example, international supporters of Iranian protestors changed their Twitter locations to Tehran in an effort to overwhelm Iranian government censors seeking to find and punish actual Iranians who were sending out antiregime messages (Terdiman 2009).

Zhao and Sui (2017) provided a summary of possible motivations for *location spoofing*, which they defined as the intentional falsification of one's actual location. The authors proposed spoofing as a neutral term, one that encompasses motivations as benign as curiosity and privacy protection to as malicious as criminal intent and cyberespionage, acknowledging that the connotation of spoofing is traditionally negative. In the field of information security, spoofing is characterized as a technique used to gain unauthorized access through deceitful impersonation (Whitman and Mattord 2018). We differentiate personal location masking from location spoofing in that the goal is not necessarily to provide false location for some gain but to make the individual's actual location more difficult or impossible to ascertain. Personal location masking is more closely aligned with a collection of strategies for protecting geoprivacy.

Privacy Surveys

Previous social research on privacy has most frequently involved the deployment of surveys. Often, there is a strong dichotomy between self-reported privacy attitudes and measured privacy behaviors. Although most individuals express concern about their personal information privacy, few take any steps to protect it (Acquisti and Grossklags 2004). This finding is seconded by the recent Pew Research Center work on privacy and security attitudes (Madden and Rainie 2015). Part of the reason is that the mention of the word *privacy* can inflate self-reported concerns due to social desirability bias (Ruel, Wagner, and Gillespie 2015), as respondents might feel that privacy is important to those conducting the survey. To avoid this bias, some researchers recommend removing all mention of the word *privacy* when measuring related behaviors and attitudes (van de Garde-Perik et al. 2008).

Location privacy is much less frequently studied than general information privacy, presenting a major gap in the literature. Keßler and McKenzie (2018)

argued that location privacy is a special case of information privacy, in part due to the pervasiveness of location-collecting technology and the unforeseen inferences that can be drawn from location. The propensity to share location, rather than mask it, has received some attention from researchers. A survey of users of the Chinese social networking site RenRen found that privacy is often in competition with users' motivations to disclose location (Li et al. 2013). A related study found that social influence has a strong effect on student use of location-sharing applications (Beldad and Citra Kusumadewi 2015). Motivations for checking in with location on Foursquare include safety, coordination with friends, self-presentation, and a fondness for its gamified aspects (Lindqvist et al. 2011).

More closely related to this study is work on public perceptions of location privacy specifically related to online crime mapping (Kounadi, Bowers, and Leitner 2014). The importance that individuals place on geoprivacy in more routine activities is still unknown, however. Another survey (Kar, Crowsey, and Zale 2012) examined attitudes toward location privacy in the United States but was limited to snowball sampling of geography students and GIS professionals. Another survey of geography university students found that the majority of respondents did not contribute VGI on smartphones due to privacy concerns (Ricker, Schuurman, and Kessler 2015). In a more related study with university students, Leszczynski (2015) found that 68 percent of respondents paid attention to whether smartphone applications requested permission to access location, and 52 percent routinely interacted with location services controls, enabling location services in some cases and shutting them down in others. Outside of university students, there is a large research gap when it comes to public attitudes and behaviors regarding geoprivacy. This study fills that gap by deploying a statewide California survey examining (1) the prevalence of personal location masking behavior and (2) its connection to geoprivacy-related knowledge and attitudes.

Conceptualization

Pursuant to these goals, this study employed the knowledge–attitudes–behavior model to explain personal location masking by Internet users, a model commonly used to predict human behavior in health

and environmental studies (Morgan and Miller 2002; Levine and Strube 2012). This model hypothesizes that an increase in knowledge about a phenomenon causes changes in attitudes, which accumulates into behavior change. In this case, greater knowledge about the pervasiveness of location collection is hypothesized as correlated with more concerned privacy attitudes and higher levels of personal location masking behavior. Hypothesized background variables included education level, age, sex, income, ethnicity, and rural location (Figure 1). Previous work found that those with higher education levels were more likely to support anonymous Internet browsing (Madden and Rainie 2015), and those with lower education were less familiar with location privacy regulations (Kar, Crowsey, and Zale 2012). Age was another anticipated predictor; younger adults have been found more likely to support stricter, more protective definitions of location privacy (Kounadi, Bowers, and Leitner 2014), provide inaccurate information online (Madden and Rainie 2015), and use strategies to protect online privacy (Yang and Liu 2014). In some studies, sex was found not to influence privacy attitudes and behaviors, but Kar, Crowsey, and Zale (2012) found that women are more likely to deem it a privacy violation if a commercial firm takes pictures of one's home. Lower income has been found to be significantly correlated with lower privacy concerns (Acquisti and Grossklags 2004). Finally, it was expected that traditionally marginalized groups would exhibit less trust in personal information exchanges, including location sharing. Therefore, location masking behavior was expected to vary by ethnicity. Finally, a recent study found that users in rural California regions were more likely to deliberately mask location when

posting an advertisement on Craigslist (Seidl and Allen 2016).

Intervening variables for masking behavior were expected to include experience with identity theft, hacking, or other privacy infringement; data industry experience; and lower enjoyment of social media. A recent privacy infringement was expected to result in decreased trust and greater suspicion of data collection authorities, as well as stronger support for geoprivacy. For example, a previous negative experience in online information disclosure increases privacy concern and perceived risk in sharing on social media (Yang and Liu 2014). Likewise, employment in a data collection or data science industry was expected to result in heightened knowledge of geoprivacy issues and thus higher concern and greater personal location masking. Examining the intervening variable of social media enjoyment, Lindqvist et al. (2011) found that users of Foursquare had few concerns about privacy.

Methods

This study employed an online questionnaire to measure geoprivacy attitudes and their relation to online masking behavior. The target population was adult Internet users in California, a state with a strong tradition of privacy and a diversity of rural and urban populations. California's state constitution promises an inalienable right to pursue and obtain privacy, and the 2015 passage of the California Electronic Communications Privacy Act (CalECPA) further protects digital privacy by restricting government from accessing electronic data without a warrant. The California Consumer Privacy Act (CCPA), which goes into effect in 2020, requires companies to inform consumers of data collected about them and allow them to opt out of its sale. High-speed home Internet access among Californians is at an above-average 80.5 percent of households, compared to the national average of 78.0 percent (File and Camille 2014), which is helpful for an Internet-based survey. Strong practices of Internet use in the study area were expected to result in a higher response rate.

Questionnaire Design

A primary concern in the questionnaire design was to avoid participant overreporting of privacy

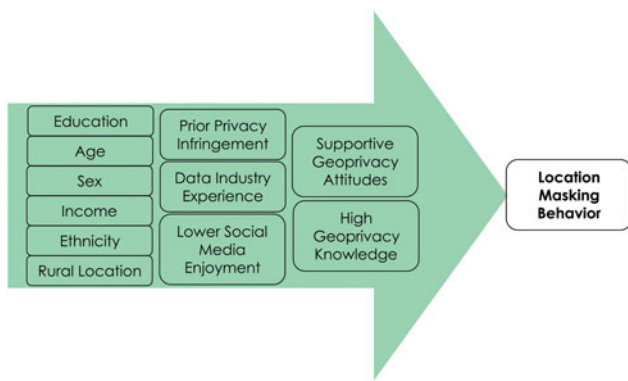


Figure 1. Conceptual model of hypothesized predictors of masking behavior.

concerns and to measure personal location masking behavior as it would take place in a routine online setting. To avoid the response bias (Ruel, Wagner, and Gillespie 2015) anticipated from advertising the topic of the study as location privacy, this study used incomplete disclosure with institutional review board (IRB) approval and advertised the questionnaire as a “Study of Online Information Sharing.” The word privacy was not used until the completion of the survey, when the full purpose of the study was revealed. Participants at this point had the opportunity to withdraw their responses.

The primary test of location masking took place within the first survey question. Before questionnaire items addressing geoprivacy attitudes and behaviors, respondents were asked to provide a home location within the fields of street, cross-street, city, state (prefilled for California), and ZIP code (Figure 2). Participants could then adjust their location in a map interface by moving a pin that was initially placed at the geocoded home location using the Google geocoding application programming interface. This setup was designed to simulate the location prompts involved with posting a classified advertisement on Craigslist. Craigslist users are encouraged to enter a location and then adjust the point in a map interface, presumably to make any corrections to the geocoded location. Both of these questions were optional; participants had complete control over how much location information to provide and whether to move the map pin. Respondents then indicated their level of agreement on a five-point Likert scale (*strongly disagree* to *strongly agree*) to the statements, “I intentionally provided incorrect information on my home location,” and “I intentionally moved the pin on the map away

from my home location.” The remainder of the survey consisted of similar Likert-type items, asking participants to respond with their level of agreement to additional measures of geoprivacy knowledge, attitudes, and behaviors. The survey was hosted on the Qualtrics platform, which included encryption of survey responses.

Sampling

The survey instrument was deployed to two samples within California between October 2017 and March 2018. The first, a probability sample, was drawn from an address-based sampling frame purchased from Survey Sampling International (SSI), a vendor certified to access the U.S. Postal Service (USPS) delivery sequence file, which includes households receiving mail at post office boxes. This sample included 2,000 households randomly distributed throughout California and an additional 300 households within rural census tracts, as defined by Rural–Urban Commuting Areas (RUCA) released by the U.S. Department of Agriculture (Economic Research Service 2010). This rural oversample was designed to attenuate expected selection bias from lower response rates in rural areas and ensure rural subgroups were represented (Kitchin and Tate 2013). Households in this sample were contacted by an initial postal letter invitation to the “Study of Online Information Sharing” and two follow-up postcard reminders to complete the survey online. Participants were incentivized with a \$10 Amazon.com gift card.

The second sample was an online open sample reached by Craigslist and paid Facebook advertising

Figure 2. Home location question with subsequent option to adjust map pin.

targeting adult California residents. Participants in this sample were offered a \$2 Amazon.com gift card. The online sample was expected to include different demographics than the mail sample and, in particular, be composed of participants who would be less concerned about privacy. Reaching multiple samples was intended to increase the external validity of the overall survey by increasing the sample size, ensuring that smaller subgroups were represented, and through comparison of the geoprivacy attitudes and masking behavior of the two samples (Kitchin and Tate 2013). The recruitment materials for both samples clearly stated that this survey was part of a university research project.

Analysis

Differences between the two samples, as well as differences between males and females, were evaluated with nonparametric Mann–Whitney *U* tests, appropriate for differences between two groups within a categorical variable (Ruel, Wagner, and Gillespie 2015). The Kruskal–Wallis test, another nonparametric test for a categorical input variable with more than two groups (McCarroll 2016), was used to test differences between reported ethnicities. Because the majority of questionnaire items were five-point ordinal Likert-type questions, Spearman’s correlations were suitable for calculating significant correlations between the background, intervening, and outcome location masking variables (Nolan and Heinzen 2010). Because prior privacy infringement, geoprivacy knowledge, geoprivacy attitudes, and masking behavior were captured by multiple items in the questionnaire, Cronbach’s alpha was calculated to determine whether responses demonstrated consistency within these categories (Ruel, Wagner, and Gillespie 2015). High internal consistency would support the creation of a scale variable that would summarize responses for these categories.

The outcome variables of location masking included precision of home location provided (*numbered street address to none*), agreement to “provided inaccurate home location” and “moved pin away from home location” (*strongly disagree to strongly agree*), and frequency of “use technology to alter IP address,” “provide incorrect or misleading location to retailers,” and “turn location services off on smartphone” (*never to very frequently*). Ordinal logistic regression was used to test the predictors of these ordinal variables (O’Connell 2006). The results of the Mann–Whitney *U* tests and the Spearman’s correlation matrix informed selection of predictors in the logistic regression models by helping to identify any variables that were collinear or highly correlated with behavior and therefore good candidates for inclusion.

To determine geographical patterns, kernel density maps of responses were created using a cell size of 10,000 m, a search radius of 15,000 m, and a quartic kernel. The locations used to generate the kernel density estimations were responses from the question asking participants to enter their home locations geocoded using the ArcGIS World Geocoding Service. Global and local Moran’s *I*s were applied as tests of spatial autocorrelation for survey participation rates and all survey variables. These statistics enable the detection of clusters of high masking activity or privacy concern and help to determine whether the survey response locations fall within expected thresholds for sampling.

Results

There were 214 total participants in this survey, with 113 respondents from the postal address sample and 101 from the open online sample. The open sample differed significantly from the mail sample in demographics (Table 1), but knowledge and

Table 1. Demographic results for the two samples

Variable	Mail sample	Open sample	Mann–Whitney <i>U</i> significance ($p < 0.05$)
Total participants	113	101	
Female	55%	76%	*
White	66%	55%	
Completed college	69%	44%	*
Somewhat or very urban	62%	56%	
Median age group	45–54	25–34	*
Median income tax bracket	\$38,000–92,000	\$9,000–38,000	*

attitudes related to geoprivacy were strikingly consistent between the samples. Overall, the open sample was significantly more female, less educated, younger, and had lower income than the mail sample participants in Mann–Whitney U tests ($p < 0.05$).

Background Variables

In the Mann–Whitney U tests, males and females differed in just two of the outcome variables; males were more likely to hold the privacy-protective attitude that “people should have the ability to browse the Internet completely anonymously for certain types of activities” and the masking behavior of using technology to alter IP address ($p < 0.05$). Incidentally, males had significantly higher education, age, and income levels than female respondents ($p < 0.05$), although this is likely linked to the higher proportion of females in the open sample, which overall had lower education, age, and income levels.

When tested with the Kruskal–Wallis statistic, there were no significant differences by ethnicity in the outcome variables, with the exception of self-reported geoprivacy knowledge. Respondents who identified as Hispanic or Latino were significantly more likely to agree with the statement, “I am well-informed about the ways my location can be shared online” than other groups. This did not translate

into any of the masking activity, because there were no behavioral differences by ethnicity.

Geographic Distribution

Responses from the two samples were geographically distributed throughout populated California. Figure 3 illustrates similarly distributed responses from the two groups, with the highest densities in the San Francisco Bay Area, Los Angeles, Orange County, and San Diego. Point locations for the kernel density were geocoded from participant input to the home location question. The mail sample achieved a slightly higher density in the Bay Area, whereas the open sample had a higher density of responses in Southern California. When tested with global Moran’s I at a county level and normalized by population, however, there was no spatial autocorrelation of the response locations. This suggests that both the mail and open samples were randomly distributed.

Geoprivacy Knowledge and Attitudes

Results by sample for geoprivacy-related knowledge and attitudes were very similar (Figure 4). The only item for which the two groups differed was knowledge that it is possible for Web sites to collect location using an IP address. Although both samples

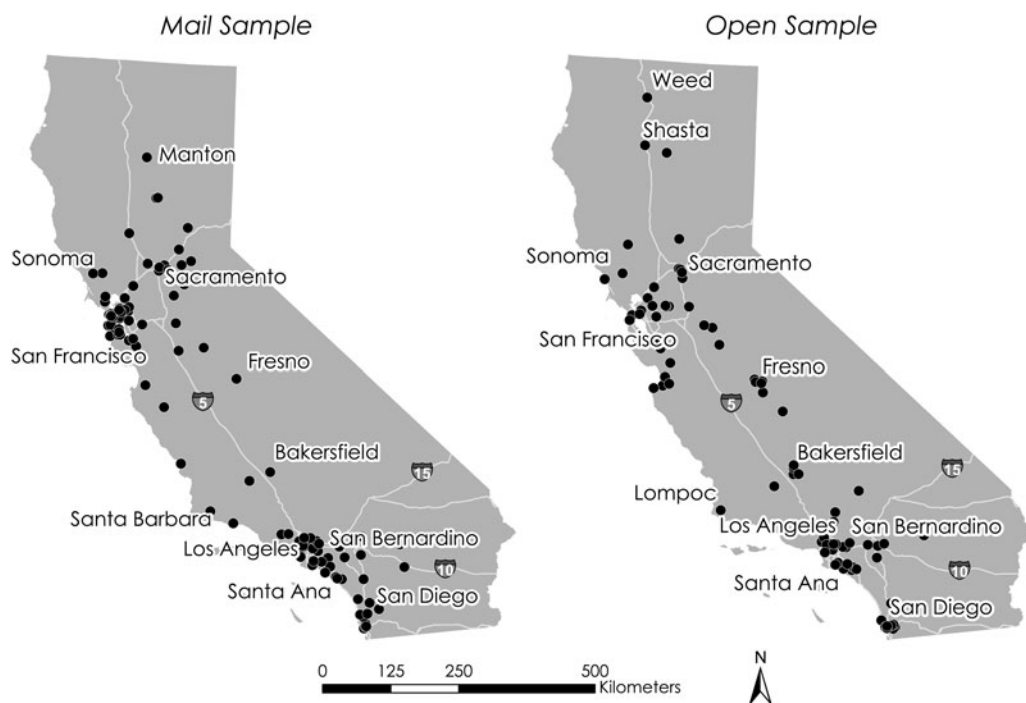


Figure 3. Maps showing distribution of survey responses in California.

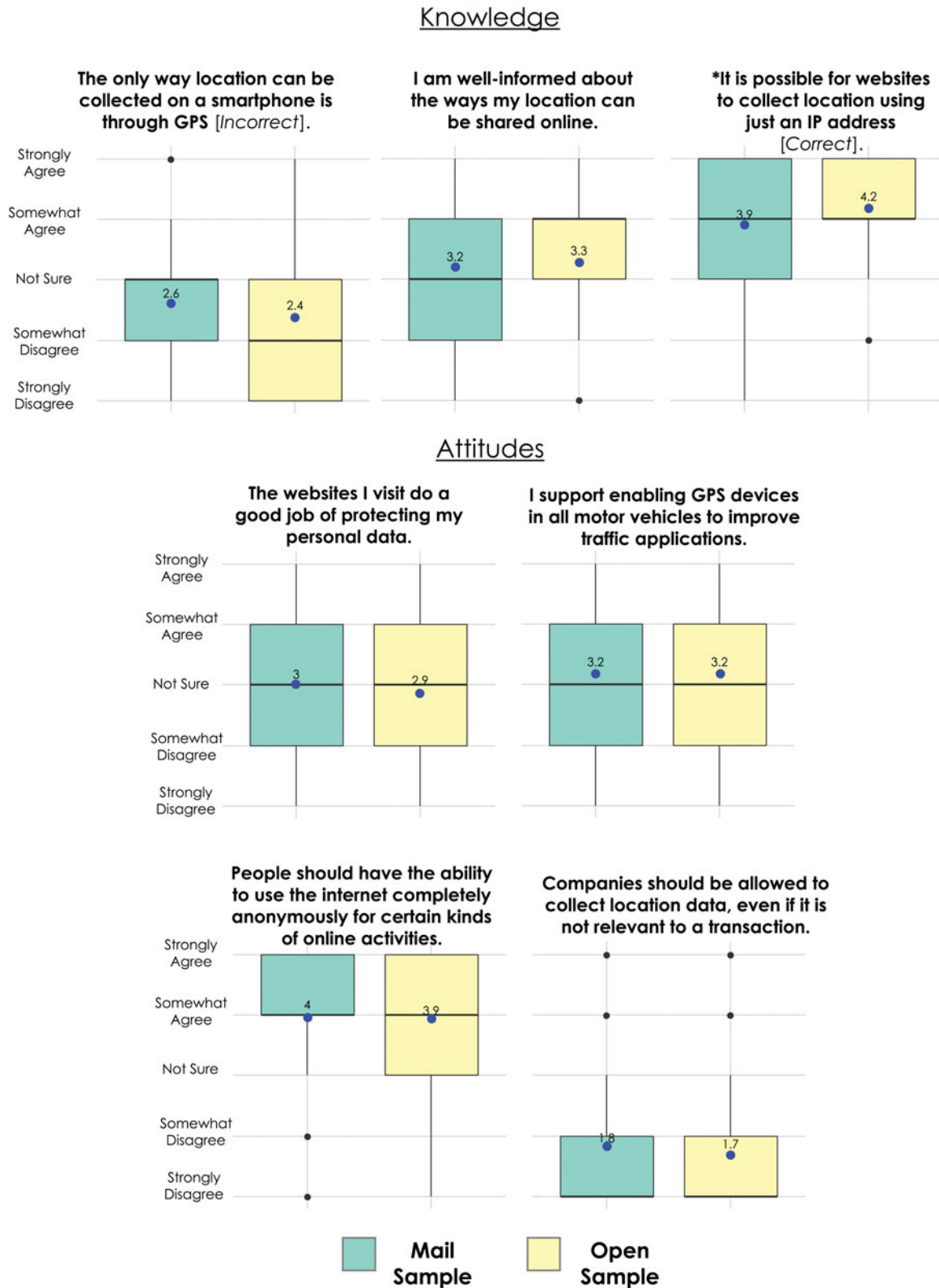


Figure 4. Box plots of geoprivacy knowledge and attitudes by sample group. *Significant difference between samples in a Mann–Whitney *U* test. GPS = Global Positioning System.

agreed overall with this statement, which is correct, the open sample was significantly more likely to agree (Mann–Whitney U test, $p < 0.05$), demonstrating higher geoprivacy knowledge. For the rest of the knowledge and attitudes variables, the two samples did not differ.

Overall, participants in this study had average knowledge of how location is transmitted and supportive attitudes toward privacy. Fifty percent of respondents somewhat or strongly disagreed (correctly) that GPS is the only way location can be collected on a smartphone, and 73 percent agreed that it is possible for Web sites to collect location from IP address. Agreement with “I am well informed about the ways my location can be shared online” was split, with 48 percent agreeing. On average, participants who knew that IP address transmits location were not sure whether smartphones collect location aside from GPS and were not sure they were well informed about location sharing.

The greatest variation in privacy attitudes between participants was for the statements “The Web sites I visit do a good job of protecting my personal data” (34 percent somewhat or strongly agreed) and “I support enabling GPS devices in all motor vehicles to improve traffic applications” (44 percent somewhat or strongly agreed). Participants generally had more privacy-protective attitudes, supporting anonymous Internet browsing (73 percent in agreement) and in disagreement with company collection of irrelevant location data in transactions (just 8 percent in support). These results were consistent between samples.

Personal Location Masking Behavior

Location masking behavior was present in all of the outcome variables and in both samples (Figure 5). A surprising proportion of respondents provided a numbered street address with city, state, and ZIP code, even though it was not required for the survey. This location disclosure was made by 73 percent of mail sample respondents and 56 percent of open sample respondents. Yet, in both samples, 15 percent of respondents somewhat or strongly agreed that they intentionally provided incorrect location information.

Two qualifiers were important for some of the masking behaviors measured: interaction with the map function for home address and smartphone ownership. Of all respondents, 70 percent moved the pin on the map, and 94 percent owned a smartphone. The mail sample respondents were significantly more likely to interact with the map function (Mann–Whitney U , $p < 0.05$), but both groups were equally likely to have a smartphone.

For map-based location masking, 11 percent of respondents who used the map function reported intentionally moving the pin away from their home locations. Of smartphone owners, 27 percent reported often or always keeping location services off, and 20 percent of these respondents had their location services off at the time they took the survey. Participants also reported providing incorrect or misleading location information to retailers (26 percent and 35 percent of mail and open sample respondents, respectively) and sometimes using technology to alter an IP address (9 percent and 26 percent of mail and open sample respondents). In Mann–Whitney U tests, participants in the open

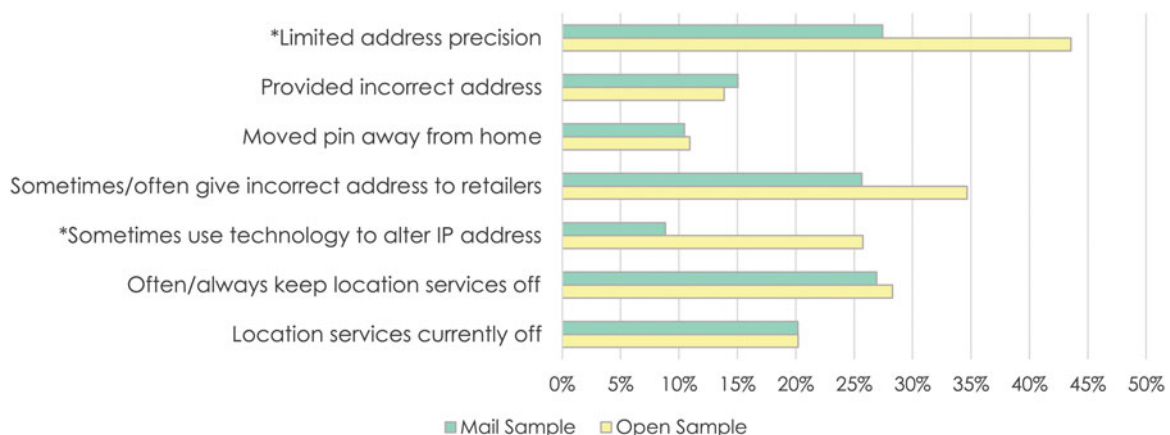


Figure 5. Percentage of participants exhibiting location masking behavior by sample group. *Significant difference between samples in a Mann–Whitney U test.

sample were significantly more likely to provide a lower precision home address and to use technology to alter an IP address (Figure 5). For the other variables, respondents engaged in masking behavior at the same rates.

Scale Variables

Given the frequency and variation in ordinal questions measuring prior privacy infringement (four items), geoprivacy knowledge (three items), privacy attitudes (four items), and masking behavior (six items), the consistency of these constructs was measured using Cronbach's alpha. In preparation for this test, variables measuring the same concept, but in reverse order, were recoded. For instance, responses to "the only way location can be collected on a smartphone is through GPS" were reversed to have higher values indicate greater geoprivacy knowledge.

The results for geoprivacy knowledge (0.29), attitudes (0.39), and behavior (0.42) revealed low internal consistency and did not support the construction of scale variables. The four items measuring previous privacy infringement, however, were highly correlated with each other. These included unauthorized user access of an online account, notification of credit or debit card fraud, identity theft experience, and information stolen in an online hacking event. The Cronbach's alpha for these variables was 0.71, which meets the threshold of 0.70 seen as adequate for combining scale items (Tavakol and Dennick 2011). Therefore, a variable for hacking experience was created, summing the results of these four responses.

Variable Correlates

The correlation matrix from the Spearman's correlations for ordinal variables is provided in Table 2.

Table 2. Spearman's correlation matrix for survey variables

Variable	B1	B2	B3	B4	I1	I2	K1	K2	K3
B1. Education	1								
B2. Age	0.36	1							
B3. Income	0.48	0.38	1						
B4. Urban location	0.26	0.14	0.23	1					
I1. Recent hacking experience	0.21	0.35	0.19	0.19	1				
I2. Social media enjoyment	-0.16	-0.04	-0.11	0.00	-0.04	1			
K1. Knowledge smartphone location	0.03	-0.20	-0.03	-0.10	0.00	0.01	1		
K2. Well-informed location sharing	-0.11	-0.23	-0.04	0.04	-0.23	0.14	0.12	1	
K3. Knowledge IP address location	-0.04	-0.14	-0.03	0.06	-0.12	0.05	0.14	0.12	1
A1. Believe Web sites do not protect data	0.24	0.08	0.18	0.09	0.25	-0.21	0.27	-0.20	0.22
A2. Against GPS in all vehicles	0.09	-0.02	0.05	-0.02	-0.06	-0.24	0.08	-0.03	-0.02
A3. Support anonymous browsing	-0.03	0.00	0.02	0.12	0.02	0.05	0.05	0.06	0.12
A4. Against location collection	0.12	0.14	0.01	0.10	0.04	0.05	0.03	-0.13	0.24
M1. Lowered home location precision	0.12	-0.07	0.03	-0.08	0.10	-0.09	0.14	-0.06	0.00
M2. Provided inaccurate address	0.03	-0.02	0.06	0.06	0.03	-0.23	-0.06	-0.06	-0.08
M3. Moved pin away from home	-0.02	-0.10	0.02	0.07	-0.07	0.12	-0.03	0.03	0.00
M4. Alter IP address	-0.03	-0.15	0.01	0.02	-0.03	-0.07	0.07	0.10	0.17
M5. Give inaccurate address to retailer	0.09	-0.26	0.02	0.10	0.09	-0.08	0.03	0.01	-0.01
M6. Turn location services off	0.06	-0.05	0.06	0.08	0.01	-0.20	-0.06	0.02	-0.04
	A1	A2	A3	A4	M1	M2	M3	M4	M5
A1. Believe Web sites do not protect data	1								
A2. Against GPS in all vehicles	0.18	1							
A3. Support anonymous browsing	0.09	0.10	1						
A4. Against location collection	0.17	0.17	0.20	1					
M1. Lowered home location precision	0.24	0.04	-0.08	0.05	1				
M2. Provided inaccurate address	0.08	0.04	0.03	-0.09	0.14	1			
M3. Moved pin away from home	0.09	0.07	-0.11	-0.11	0.04	0.41	1		
M4. Alter IP address	0.16	0.01	0.05	-0.08	0.17	0.12	0.07	1	
M5. Give inaccurate address to retailer	0.15	0.12	0.13	0.00	0.19	0.23	0.07	0.16	1
M6. Turn location services off	0.09	0.38	-0.09	-0.01	0.04	0.09	0.19	0.00	-0.02

Notes: Significant positive correlations are shown in bold; significant negative correlations are shown in bold italics ($p < 0.05$). GPS = Global Positioning System.

Variables are grouped into background (B1–4), intervening (I1–2), knowledge (K1–3), attitudes (A1–4), and masking behavior (M1–6). The background variables were positively correlated with each other; higher education was correlated with age, income, and urban location ($p < 0.05$). These variables were also positively correlated with a recent privacy infringement or hacking experience ($p < 0.05$). Data industry employment was not correlated with any outcome variables and was therefore excluded from Table 2. In general, geoprivacy knowledge and privacy-protective attitudes were positively correlated with masking behavior. The surprise in these results was K2, or self-reported knowledge of how location is shared. This knowledge indicator was not significantly correlated with masking behavior, but it was negatively correlated with the belief that Web sites do not do a good job of protecting data (-0.20). In other words, participants who believed themselves to be well informed about how location is shared also believed that the Web sites they visit do a good job of protecting personal data. This K2 variable is also negatively correlated with the hacking scale variable (I1) with a correlation of -0.23 , suggesting that a recent privacy infringement can temper confidence in one's ability to manage location data. For the other two measures of geoprivacy knowledge (K1 and K3), the relationship with the A1 variable of trust in Web sites was the opposite. Higher knowledge about how location is collected on smartphones and through IP address was positively correlated with a belief that Web sites do not do a good job of protecting data (0.27 and 0.22, respectively).

The privacy attitude most correlated with other variables was A1, the belief that Web sites do not do a good job of protecting personal data. This concerned privacy attitude was positively correlated with age, income, recent privacy infringement, smartphone location knowledge, and IP location knowledge. It also had a positive correlation with masking activity: 0.24 for lowering location precision, 0.16 for using technology to alter IP address, and 0.15 for providing inaccurate address to retailers ($p < 0.05$). A1 had a negative correlation with enjoyment of social media and self-reported knowledge of location sharing.

The correlations reveal that there is still a dichotomy between privacy-supportive attitudes and behaviors. A4, disagreement that companies should be allowed to collect irrelevant location data, is not

correlated with any of the masking behaviors, nor is A3, support for anonymous Internet browsing. A2, disagreement with enabling GPS devices in all motor vehicles, was highly and significantly correlated with M6, frequency of turning off smartphone location services (0.38), but not correlated with any other masking activity. Enjoyment of social media, a hypothesized intervening variable (I2), also had significant negative correlations with masking, including M2, providing inaccurate home address (-0.23), and M6, turning off location services (-0.20).

Masking activity was also positively correlated with itself. For instance, giving an inaccurate address to retailers (M5) was significantly positively correlated with limiting precision of home location (0.19), providing inaccurate home location (0.23), and using technology to alter IP address (0.16). Turning off location services (M6) had a significant positive correlation with moving the map pin away from the home location (0.19). Overall, the correlations demonstrate that each item in the knowledge and attitudes groups captures a somewhat different concept with complex relationships to masking behavior.

Spatial Autocorrelation

This study also measured spatial autocorrelation for the questionnaire items using global and local Moran's I . Background variables exhibiting significant global clustering were participant-reported urban index, data industry employment, and income. Geoprivacy knowledge exhibited no significant global clustering, but two privacy attitudes and one masking behavior did ($p < 0.05$). Privacy-supportive attitudes, such as lower trust in Web sites (A1) and lower support of GPS devices in all vehicles (A2), clustered in Berkeley and San Diego, whereas lower concern clustered in Central Valley cities. Use of technology to alter IP address (M4) had hot spots north of San Francisco and clusters of low values south near Modesto. No other masking behaviors exhibited spatial autocorrelation and therefore their distributions could not be distinguished from a random distribution.

Predictors of Personal Location Masking

This section presents the results of ordinal regression models predicting the six personal location

Table 3. Ordinal regression results for personal location masking outcome variables, models with lowest AIC shown

Coefficients	Value	SE	t Value	p Value	Odds ratios
M1. Limited precision of home location					
Open online sample*	0.895	0.318	2.816	0.005	2.447
Completed college	0.596	0.324	1.840	0.066	1.816
Believe Web sites do not do a good job of protecting personal data*	0.434	0.150	2.895	0.004	1.544
Provide retailers with incorrect/misleading location data*	0.425	0.157	2.700	0.007	1.530
Residual deviance: 371.93 AIC: 387.93					
M2. Provided inaccurate home location					
Enjoy contributing to social media*	-0.500	0.195	-2.563	0.010	0.606
Provide retailers with incorrect/misleading location data*	0.605	0.195	3.100	0.002	1.832
Residual deviance: 243.95 AIC: 255.95					
M3. Moved pin away from home location					
Male	-0.796	0.607	-1.312	0.190	0.451
Open online sample	0.705	0.494	1.427	0.153	2.024
Frequently turn off location services on smartphone	0.408	0.229	1.787	0.074	1.504
Residual deviance: 181.51 AIC: 195.51					
M4. Use technology to alter IP address					
Male*	1.042	0.348	2.995	0.003	2.835
Age	-0.104	0.107	-0.973	0.331	0.901
Open online sample*	1.217	0.372	3.273	0.001	3.376
Know it is possible for IP address to reveal location*	0.432	0.213	2.027	0.043	1.541
Believe Web sites do not do a good job of protecting personal data*	0.331	0.155	2.133	0.033	1.393
Residual deviance: 322.26 AIC: 338.26					
M5. Provide incorrect or misleading address to retailers					
Male*	0.554	0.281	1.974	0.048	1.740
Age*	-0.403	0.087	-4.634	0.000	0.669
Completed college*	0.699	0.289	2.423	0.015	2.012
Believe Web sites do not do a good job of protecting personal data	0.221	0.131	1.681	0.093	1.247
Residual deviance: 494.25 AIC: 510.25					
M6. Frequently turn off location services					
Male	-0.553	0.300	-1.845	0.065	0.575
Completed college	0.312	0.286	1.092	0.275	1.366
Enjoy contributing to social media	-0.118	0.164	-0.717	0.473	0.889
Do not support enabling GPS in all motor vehicles*	0.561	0.120	4.665	0.000	1.752
Residual deviance: 473.49 AIC: 489.49					

Notes: *Significant predictor variables. AIC = Akaike information criterion; GPS = Global Positioning System.

masking variables (Table 3). Initial development of these models included all possible predictor variables and was informed by the Spearman's correlation analysis and Mann-Whitney *U* tests. Models with the lowest AIC values were selected for presentation, whether or not predictor variables remained significant (Harris 2016). All of the outcome masking behaviors had relatively few remaining predictors in their models. They also had relatively high residual deviance values, suggesting that there are more factors at play in predicting masking behavior than are currently captured in this study.

Factors that remained significant in predicting a lower precision in provided address by participants (M1) were recruitment through the online sample, the belief that Web sites do not do a good job of

protecting personal data, and the additional antecedent masking behavior of providing retailers with an incorrect address. The behavior of giving retailers an incorrect address (M4) was also a significant predictor for the M2 model predicting provision of incorrect home address within the survey, as was lower enjoyment of social media. For the M3 model predicting moving a pin away from the home location, none of the modeled predictors remained significant, although frequently turning off location services was close ($p=0.07$). The factors influencing the M3 masking behavior merit more study.

For models of masking outside the survey environment (M4-6), the background variables of sex and age remained important predictors. Being male was a significant predictor of M4, using technology to alter

an IP address, and M5, providing an incorrect address to retailers. Age and completing college were also significant predictors of M5. The only variable that remained a significant predictor of M6, frequency of turning off location services, was the attitude of not supporting GPS in all motor vehicles. Only one knowledge variable was a significant predictor of masking behavior; use of technology to alter an IP address was successfully predicted by knowledge that an IP address transmits location. The most consistent significant attitudinal predictor of masking behavior was A1, the belief that Web sites do not do a good job of protecting personal data, which predicted M1 and M4 and remained in the model for M5. On the whole, the knowledge and attitude predictors of masking are closely related to the context of the masking behavior; IP address knowledge predicts IP masking, Web site privacy attitudes predict online masking, and GPS attitudes predict nonuse of location services.

Discussion

Overall, the study results indicate that individuals across demographic groups participate in personal location masking. There is evidence for all of the following masking activities tested in our survey: providing an incorrect address, limiting address precision, moving a map pin away from the home location, providing an incorrect address to retailers, turning off location services, and using technology to alter an IP address. The prevalence of location masking ties in with Leszczynski's (2015) concept of "anxieties of control" describing the public's response to geoprivacy challenges. Personal location masking and its demonstrated link to knowledge and attitudes about privacy in this survey lend support to the idea that data anxieties operate at the level of devices and applications, or the entry points for location collection. In addition to location collection by networked devices, this study suggests that there may be data control anxiety at the entry point of manually entering a home location in text fields.

Although we did not measure respondents' motivations for turning off location services, this study finds that 27 percent of respondents reported often or always keeping smartphone location services off. Our study measured this personal masking activity in a different manner than Leszczynski's (2015) survey of university students, which reported that just over

half of respondents actively toggled location services on and off. Although we have framed toggling location services as a personal masking activity, corporate and government actors continue to capture device locations through cell tower triangulation, WiFi probe requests, and Bluetooth. In that regard, exercising control over data flows at the location services level might offer protection only in that it eliminates one of the more accurate tracking mechanisms: GPS. Otherwise, there remain other components of the linked network ecology of big data (Marwick and Boyd 2014) with which it is possible to capture and distribute personal location data.

Despite evidence for personal masking behavior, 73 percent of the mail sample and 56 percent of the open sample provided the highest precision of home location: a numbered street address with city and ZIP code. This result differed significantly between samples, suggesting that context has an impact on personal location masking. Because the address-based sample was recruited by mail, this group either recognized that this project already had home address data or had more trust in the overall study due to the printed contact materials. Contact materials for both samples made it evident that this was a university-sponsored research project. Open sample participants might have had less trust in the Internet-based advertising of the survey. Another possibility is that the lower monetary incentive offered to open sample participants was too low to encourage participants to provide their home addresses. Open sample participants received \$2, whereas mail sample participants received \$10. This would support previous research that the price of location privacy, measured by the minimum compensation that participants would require to participate in a month-long location tracking study, is \$13 (Danezis, Lewis, and Anderson 2005).

The results of this survey corroborate recent calls for increased education on geoprivacy mechanisms as resistance to surveillance. Swanlund and Schuurman (2016) described how education in the technical language of geosurveillance mechanisms is essential to maintaining agency against them. As part of their geoprivacy manifesto, Keßler and McKenzie (2018) called for public education in LBS to engage users in negotiating location privacy with service providers. Supporting these arguments, this study finds that geoprivacy knowledge is correlated with the masking behaviors of limiting address precision and altering IP address. Being male and part of the online sample

were also significant predictors for masking IP address. These groups are perhaps more likely to engage with the technocratic language needed to enact IP masking. Incidentally, the measurement of IP masking did not test if this was due to use of a virtual private network (VPN) for employment purposes or an active strategy to hide location. Future efforts should stress the difference between these purposes. Although there is no guarantee that the returned location is correct, IP address is commonly used to look up location. It is also possible that participants who had knowledge that an IP address can be used to identify location found it futile to mask location when asked for a home address or to move a map pin. This might explain why this study did not find correlations between education and personal location masking.

This study used self-reported knowledge about how location is shared as an indicator of knowledge. The results suggest that this construct is better suited as a measure of geoprivacy attitudes, rather than knowledge, because it was not consistent with the other knowledge variables. Participants who felt well informed were not those who scored well on the other tests of technical geoprivacy knowledge. In addition, self-reported knowledge was positively correlated with trust in Web sites to protect personal data, whereas the other knowledge variables had negative correlations with this attitude. Self-reported knowledge was negatively correlated with a recent hacking experience, suggesting that privacy infringement lowers confidence in one's agency to manage privacy. This result supports other recent findings on low public awareness of the extent of personal data collection (Raine 2016).

The most common masking behavior captured in this study was the provision of incorrect or misleading address data to retailers, with 26 percent and 35 percent of mail and open sample respondents, respectively, sometimes or often masking in this way. This information, as well as the statistic that 15 percent of survey respondents reported giving an incorrect address in the survey, can be helpful in generating error estimates for future studies that attempt to capture location. These results also demonstrate the importance of context in personal masking behavior. Personal location masking appears more prevalent when the recipient of location data is a retailer, rather than university researchers. It is possible that respondents put more trust in the

university affiliation of the survey than with retailers and therefore reported contributing more accurate home locations. In related work, trust has been reported as a main predictor of adoption of location sharing applications (Beldad and Citra Kusumadewi 2015). Similarly, a key attitude predicting masking behavior was the belief that Web sites do a good job of protecting personal data. Respondents who disagreed with this statement were more likely to provide a lower precision of home address, alter IP address, and give inaccurate address information to retailers.

In the decision to participate in personal location masking, consumers might also be conducting a cost-benefit analysis (Danezis, Lewis, and Anderson 2005). Internet users might divulge their locations to obtain some benefit, such as use of a free online service or application to search for nearby restaurants or directions to the nearest gas station. In a similar vein, consumers might weigh these benefits against the cost of compromising location privacy. It is possible that participants in this survey varied the precision and accuracy of their reported home location according to anticipated benefits of completing the survey, such as the incentive payment. Participants might have been more likely to report a correct and precise home address if they perceived their gift card delivery to be contingent on correct home address, although incentive payments were delivered electronically. A lack of incentive payments in a new iteration of this survey might result in greater masking activity if participants perceive no benefit in providing a correct location.

Extensions of this survey research should also evaluate direct motivations behind different masking behaviors. As mentioned in the Introduction, some Internet users alter their locations not to protect privacy but to gain other benefits. For example, participants in the game Pokémon Go have been documented to spoof location to obtain game rewards (Zhao and Chen 2017), and other motivations for location spoofing include curiosity, research interests, social rewards, or criminal activity (Zhao and Sui 2017). This study only asked respondents about the frequency with which they altered their IP addresses but not the motivations behind this activity.

This survey had the unusual property of asking respondents to report on their honesty in providing their home locations, both through text and by moving a point on the map. In both the mail sample and the open sample, 15 percent of respondents

reported providing incorrect address information. This calls into question whether or not respondents provided correct information for other survey variables, such as age, income, or education level. It is possible that the survey achieved similar rates of respondent misreporting of demographic variables, although there was no means to test for this in the survey.

Conclusion

This study fills a major gap in the privacy literature by focusing on public attitudes and behaviors related to geoprivacy. Most research on privacy with human subjects fails to recognize the power of identifying location, and studies of public attitudes toward geoprivacy have heretofore been limited. Although the population for this study is in California, the methodology could be replicated in other regions. This study finds that 15 percent of Internet users asked to enter a home address provide incorrect location information, and 10 percent of those moving a pin on the map move it away from their home locations. This masking behavior takes place across social lines by both males and females, across ethnic groups, and across income levels. Furthermore, these might be underestimates of location masking; in this study, participants had to admit that they intentionally provided incorrect location, because no ground truth of location was collected from IP address. It is possible that some respondents were unwilling to reveal that they had provided inaccurate locations, particularly if they feared not receiving the incentive.

A key finding of this research is that personal location masking is linked to knowledge and attitudes about geoprivacy. The belief that Web sites do not do a good job of protecting data is significantly correlated with three masking behaviors: lowering location precision, altering IP address, and providing inaccurate address to retailers. Knowledge that it is possible for IP address to reveal location is a significant predictor of IP address masking, and a lack of support for GPS devices to be enabled in all motor vehicles is a significant predictor of turning off smartphone location services.

In highlighting the privacy protection strategies of Internet users, this work demonstrates that despite pervasive data collection, individuals can play a role in protecting their location privacy. Still, personal location masking is practiced by a minority of

Internet users in a state with a large high-technology sector and a protected right to electronic privacy. It is recommended that this study be extended beyond California to capture a better sense of the prevalence of geoprivacy attitudes and behaviors.

Acknowledgment

We thank Krzysztof Janowicz for his comments and suggestions, which contributed greatly to this work.

Supplemental Material

The full text of the survey instrument employed in this study can be accessed on the [publisher's Web site](#).

ORCID

Dara E. Seidl  <http://orcid.org/0000-0001-8737-7115>

Piotr Jankowski  <http://orcid.org/0000-0002-6303-6217>

Keith C. Clarke  <http://orcid.org/0000-0001-5805-6056>

Atsushi Nara  <http://orcid.org/0000-0003-4173-7773>

References

- Acquisti, A., and J. Grossklags. 2004. Privacy attitudes and privacy behavior. In *Economics of information security*, ed. L. J. Camp and S. Lewis, 165–78. Boston: Springer. doi: [10.1007/1-4020-8090-5_13](https://doi.org/10.1007/1-4020-8090-5_13).
- Armstrong, M. P., G. Rushton, and D. L. Zimmerman. 1999. Geographically masking health data to preserve confidentiality. *Statistics in Medicine* 18 (5):497–525. doi: [10.1002/\(SICI\)1097-0258\(19990315\)18:5<497::AID-SIM45>3.0.CO;2-#](https://doi.org/10.1002/(SICI)1097-0258(19990315)18:5<497::AID-SIM45>3.0.CO;2-#).
- Barry, K. 2018. Will your smartphone replace your car key? *Consumer Reports*, April 5. Accessed April 8, 2019. <https://www.consumerreports.org/automotive-technology/will-your-smartphone-replace-your-car-key-virtual-key/>.
- Beldad, A., and M. Citra Kusumadewi. 2015. Here's my location, for your information: The impact of trust, benefits, and social influence on location sharing application use among Indonesian university students. *Computers in Human Behavior* 49:102–10. doi: [10.1016/j.chb.2015.02.047](https://doi.org/10.1016/j.chb.2015.02.047).
- Brunton, F., and H. Nissenbaum. 2015. *Obfuscation: A user's guide for privacy and protest*. Cambridge, MA: The MIT Press.

- Clarke, K. C. 2015. A multiscale masking method for point geographic data. *International Journal of Geographical Information Science* 30 (2):300–315. doi: 10.1080/13658816.2015.1085540.
- Council of Advisors on Science and Technology. 2014. Big data and privacy: A technological perspective. Accessed July 21, 2018. https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.
- Cox, J. 2019. Hundreds of bounty hunters had access to AT&T, T-Mobile, and Sprint customer location data for years. *Motherboard*, February 6. Accessed March 19, 2019. https://motherboard.vice.com/en_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years.
- Crawford, K. 2014. The anxieties of big data. Accessed March 19, 2019. <https://thenewinquiry.com/the-anxieties-of-big-data/>.
- Curry, M. 1997. Digital people, digital places: Rethinking privacy in a world of geographic information. *Ethics & Behavior* 7 (3):253–63. doi: 10.1207/s15327019eb0703_7.
- Danezis, G., S. Lewis, and R. Anderson. 2005. How much is location privacy worth? *Proceedings of the Workshop on the Economics of Information Security Series (WEIS)* 5:1–13.
- Dobson, J. E., and P. F. Fisher. 2003. Geoslavery. *IEEE Technology and Society Magazine* 22 (1):47–52. doi: 10.1109/MTAS.2003.1188276.
- Dobson, J. E., and P. F. Fisher. 2007. The panopticon's changing geography. *Geographical Review* 97 (3): 307–23. doi: 10.1111/j.1931-0846.2007.tb00508.x.
- Duckham, M., and L. Kulik. 2006. Location privacy and location-aware computing. In *Dynamic & mobile GIS: Investigating change in space and time*, ed. R. Billen, E. Joao, and D. Forrest, 35–51. Boca Raton, FL: CRC Press.
- Dwork, C. 2006. Differential privacy. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming*, ed. M. Bugliese, M. Preneel, V. Sassone, and I. Wegener, 1–12. Berlin: Springer. doi: 10.1007/11787006_1.
- Economic Research Service. 2010. Rural–Urban Commuting Area (RUCA) codes. Accessed July 21, 2018. <https://www.ers.usda.gov/data-products/rural-urban-commuting-area-codes/documentation/>.
- European Union. 2016. *General Data Protection Regulation (EU) 2016/679*.
- File, T., and R. Camille. 2014. *Computer and Internet use in the United States: 2013*. Washington, DC: U.S. Census Bureau. Accessed July 21, 2018. <http://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf>.
- Goss, J. 1995. We know who you are and we know where you live: The instrumental rationality of geodemographic systems. *Economic Geography* 71 (2):171–98. doi: 10.2307/144357.
- Hampton, K. H., M. K. Fitch, W. B. Allshouse, I. A. Doherty, D. C. Gesink, P. A. Leone, M. L. Serre, and W. C. Miller. 2010. Mapping health data: Improved privacy protection with donut method geomasking. *American Journal of Epidemiology* 172 (9):1062–69. doi: 10.1093/aje/kwq248.
- Harris, R. 2016. *Quantitative geography: The basics*. London: Sage.
- Hern, A. 2014. What is Apple's iBeacon? *The Guardian*, January 13. Accessed March 19, 2019. <https://www.theguardian.com/technology/2014/jan/13/what-is-apple-ibeacon-retail-tracking>.
- Hill, K. 2016. How an internet mapping glitch turned a random Kansas farm into a digital hell. Accessed March 20, 2019. <https://splinternews.com/how-an-internet-mapping-glitch-turned-a-random-kansas-f-1793856052>.
- Hill, K. 2019. How cartographers for the U.S. military inadvertently created a house of horrors in South Africa. Accessed March 20, 2019. <https://gizmodo.com/how-cartographers-for-the-u-s-military-inadvertently-c-1830758394>.
- Kar, B., R. C. Crowsey, and J. J. Zale. 2012. The myth of location privacy in the United States: Surveyed attitude versus current practices. *The Professional Geographer* 65 (1):47–64. doi: 10.1080/00330124.2012.658725.
- Keßler, C., and G. McKenzie. 2018. A geoprivacy manifesto. *Transactions in GIS* 22 (1):3–19. doi: 10.1111/tgis.12305.
- Kitchin, R., and N. Tate. 2013. *Conducting research in human geography: Theory, methodology and practice*. London and New York: Routledge.
- Kofman, A. 2019. Silent shout. *Real Life*, January 7. Accessed March 19, 2019. <https://reallifemag.com/silent-shout/>.
- Kounadi, O., K. Bowers, and M. Leitner. 2014. Crime mapping on-line: Public perception of privacy issues. *European Journal on Criminal Policy and Research* 21 (1):167–90. doi: 10.1007/s10610-014-9248-4.
- Kwan, M.-P., I. Casas, and B. Schmitz. 2004. Protection of geoprivacy and accuracy of spatial information: How effective are geographical masks? *Cartographica: The International Journal for Geographic Information and Geovisualization* 39 (2):15–28. doi: 10.3138/X204-4223-57MK-8273.
- Leszczynski, A. 2015. Spatial big data and anxieties of control. *Environment and Planning D: Society and Space* 33 (6):965–84. doi: 10.1177/0263775815595814.
- Levine, D. S., and M. J. Strube. 2012. Environmental attitudes, knowledge, intentions and behaviors among college students. *The Journal of Social Psychology* 152 (3):308–26. doi: 10.1080/00224545.2011.604363.
- Li, J., C. Zhong, Z. Cao, W. Pei, and X. Zhou. 2013. Examining privacy concern in social-driven location sharing: An empirical study on Chinese popular SNSs. In *Computer Software and Applications Conference (COMPSAC)*, 668–77. New York: IEEE. doi: 10.1109/COMPSAC.2013.106.
- Liao, S. 2017. Google admits it tracked user location data even when the setting was turned off. *The Verge*, November 21. Accessed July 21, 2018. <https://www.theverge.com/2017/11/21/16684818/google-location-tracking-cell-tower-data-android-os-firebase-privacy>.
- Lindqvist, J., J. Cranshaw, J. Wiese, J. Hong, and J. Zimmerman. 2011. I'm the mayor of my house: Examining why people use Foursquare—A social-driven location sharing application. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems—CHI '11*, 2409–18. New York: ACM. doi: 10.1145/1978942.1979295.

- Madden, M., and L. Rainie. 2015. Americans' attitudes about privacy, security and surveillance. Accessed July 21, 2018. <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.
- Marwick, A. E., and D. Boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16 (7):1051–67. doi: 10.1177/1461444814543995.
- McCarroll, D. 2016. *Simple statistical tests for geography*. Boca Raton, FL: CRC Press.
- Michalevsky, Y., G. Nakibly, A. Schulman, and D. Boneh. 2015. PowerSpy: Location tracking using mobile device power analysis. Paper presented at 24th USENIX Security Symposium, Washington, DC, August.
- Morgan, S., and J. Miller. 2002. Communicating about gifts of life: The effect of knowledge, attitudes, and altruism on behavior and behavioral intentions regarding organ donation. *Journal of Applied Communication Research* 30 (2):163–78. doi: 10.1080/00909880216580.
- National Science and Technology Council. 2016. National privacy research strategy. Accessed July 21, 2018. <https://www.nitrd.gov/PUBS/NationalPrivacyResearchStrategy.pdf>.
- Nissenbaum, H. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.
- Nolan, S. A., and T. Heinzen. 2010. *Essentials of statistics for the behavioral sciences*. New York: Worth.
- O'Connell, A. A. 2006. *Logistic regression models for ordinal response variables*. Thousand Oaks, CA: Sage.
- Puente, K. 2016. Maintenance man pleads guilty to using Instagram to burglarize 33 O.C. college students. *The Orange County Register*, September 20. Accessed July 21, 2018. <https://www.ocregister.com/2016/09/20/maintenance-man-pleads-guilty-to-using-instagram-to-burglarize-33-oc-college-students/>.
- Raine, L. 2016. The state of privacy in post-Snowden America. Accessed July 21, 2018. <http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>.
- Ricker, B., N. Schuurman, and F. Kessler. 2015. Implications of smartphone usage on privacy and spatial cognition: Academic literature and public perceptions. *GeoJournal* 80 (5):637–52. doi: 10.1007/s10708-014-9568-4.
- Ruel, E. E., W. E. Wagner, and B. J. Gillespie. 2015. *The practice of survey research: Theory and applications*. Los Angeles: Sage.
- Scism, L. 2016. Car insurers find tracking devices are a tough sell. *Wall Street Journal*, January 10. Accessed July 21, 2018. <http://www.wsj.com/articles/car-insurers-find-tracking-devices-are-a-tough-sell-1452476714>.
- Seidl, D. E., and C. Allen. 2016. *Unlisted: Variations in location sharing by Craigslist users*. Albuquerque, NM: CaGIS. Accessed July 21, 2018. http://geo.gmu.edu/AutoCarto2016/Seidl_and_Allen.pdf.
- Seidl, D. E., P. Jankowski, and M.-H. Tsou. 2016. Privacy and spatial pattern preservation in masked GPS trajectory data. *International Journal of Geographical Information Science* 30 (4):785–800. doi: 10.1080/13658816.2015.1101767.
- Seidl, D. E., G. Paulus, P. Jankowski, and M. Regenfelder. 2015. Spatial obfuscation methods for privacy protection of household-level data. *Applied Geography* 63:253–63. doi: 10.1016/j.apgeog.2015.07.001.
- Shahani, A. 2014. Smartphones are used to stalk, control domestic abuse victims. *All Tech Considered*, National Public Radio, September 15. Accessed July 21, 2018. <https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims>.
- Solove, D. J. 2007. "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review* 44:1–23.
- Swanlund, D., and N. Schuurman. 2016. Mechanism matters: Data production for geosurveillance. *Annals of the American Association of Geographers* 106 (5):1063–78. doi: 10.1080/24694452.2016.1188680.
- Swedberg, C. 2019. NFC makes smartphones the key to Hyundai's new cars. *RFID Journal*, March 6. Accessed March 20, 2019. <https://www.rfidjournal.com/articles/view?18381>.
- Tavakol, M., and R. Dennick. 2011. Making sense of Cronbach's alpha. *International Journal of Medical Education* 2:53–55. doi: 10.5116/ijme.4dfb.8dfd.
- Terdiman, D. 2009. Twitterverse working to confuse Iranian censors. Accessed July 1, 2019. <https://www.cnet.com/news/twitterverse-working-to-confuse-iranian-censors/>.
- van de Garde-Perik, E., P. Markopoulos, B. de Ruyter, B. Eggen, and W. Ijsselstein. 2008. Investigating privacy attitudes and behavior in relation to personalization. *Social Science Computer Review* 26 (1):20–43. doi: 10.1177/0894439307307682.
- Whitman, M. E., and H. J. Mattord. 2018. *Principles of information security*. South Melbourne, Australia: Cengage Learning.
- Yang, H., and H. Liu. 2014. Prior negative experience of online disclosure, privacy concerns, and regulatory support in Chinese social media. *Chinese Journal of Communication* 7 (1):40–59. doi: 10.1080/17544750.2013.816756.
- Zandbergen, P. A. 2014. Ensuring confidentiality of geocoded health data: Assessing geographic masking strategies for individual-level data. *Advances in Medicine* 2014:1–14. doi: 10.1155/2014/567049.
- Zhang, S., S. M. Friendschuh, K. Lenzer, and P. A. Zandbergen. 2016. The location swapping method for geomasking. *Cartography and Geographic Information Science* 44 (1):22–34. doi: 10.1080/15230406.2015.1095655.
- Zhao, B., and Q. Chen. 2017. Location spoofing in a location-based game: A case study of Pokémon Go. In *Advances in cartography and GIScience*, ed. M. P. Peterson, 21–32. Springer. doi: 10.1007/978-3-319-57336-6_2.
- Zhao, B., and D. Z. Sui. 2017. True lies in geospatial big data: Detecting location spoofing in social media. *Annals of GIS* 23 (1):1–14. doi: 10.1080/19475683.2017.1280536.

DARA E. SEIDL is a graduate of the joint doctoral program in geography between San Diego State University, San Diego, CA 92182-4493, and the University of California, Santa Barbara. E-mail: dara.seidl@gmail.com. Her research interests include geoprivacy, spatiotemporal data analytics, and geographic information science.

PIOTR JANKOWSKI is a Professor in the Department of Geography at San Diego State University, San Diego, CA 92182-4493. E-mail: pjankows@sdsu.edu. He is also a visiting professor at Adam Mickiewicz University in Poznan, Poland. His research interests include spatial decision support systems, public participation GIS methods, and uncertainty in spatial models.

KEITH C. CLARKE is Professor of Geography in the Department of Geography at the University of California, Santa Barbara, Santa Barbara, CA 93106-4060. E-mail: kclarke@geog.ucsb.edu. His research covers the fields of cartography, geographic information science, remote sensing and geocomputation.

ATSUSHI NARA is an Associate Professor in the Department of Geography at San Diego State University, San Diego, CA 92182-4493. E-mail: anara@sdsu.edu. His research interests focus on geographic information science, spatiotemporal data analytics, geocomputation approaches, and complex adaptive systems applied to study human mobility, urban dynamics, and interdisciplinary fields.