Received: 17 January 2022 | Revised: 1 March 2022 | Accepted: 3 March 2022

DOI: 10.1111/tgis.12924

RESEARCH ARTICLE

Transactions in GIS WILEY

PrivyTo: A privacy-preserving location-sharing platform

Grant McKenzie | Daniel Romm | Hongyu Zhang | Mikael Brunila

Platial Analysis Lab, Department of Geography, McGill University, Montreal, Canada

Correspondence
Grant McKenzie, Platial Analysis Lab, Department of Geography, McGill University, Montréal, Quebec, Canada.
Email: grant.mckenzie@mcgill.ca

Funding information
Canadian Internet Registration Authority; Fonds de Recherche du Québec-Société et Culture

Abstract

Concern over the privacy of our personal location is at an all-time high, yet the desire to share our lives with friends, family, and the public persists. Current methods and applications for sharing location content with the range of people in our lives are sorely lacking. Application users are often limited to sharing a single spatial resolution with all individuals, regardless of relation, and with little control over how this content is shared. Processes for sharing typically involve allowing a for-profit company access to one's location before it can be transmitted to the intended recipient. In this work we propose a set of design goals and a design pattern for sharing personal location information that are realized through a prototype mobile web application. Our approach is built on the novel idea of obfuscated and encrypted location views, and promotes a uniquely open method for sharing. The intention of this article is to demonstrate that location sharing need not require one to expose private location information to third parties, and that methods exist to put an individual back in control of their content.

1 | INTRODUCTION

Personal data privacy is a topic of appreciable concern and confusion in today's digital society. With our increased reliance on mobile devices, and technical advances in context-aware technology, location information has become ubiquitous. Unease related to the privacy of location information has risen dramatically in recent years, pushing the discussion into the mainstream media (Warzel & Thompson, 2021). Existing work on this topic widely recognizes that the resulting social implications will substantially change our understanding of privacy in the long term

(Bohn, Coroamă, Langheinrich, Mattern, & Rohs, 2005; Weber, 2010). In fact, we are already seeing this change, as one's personal location details are now often used as a commodity to be traded for services (e.g., navigation applications, localized search, and reward programs) (Gambs, 2018). Services constantly ask users to *share their location* via their mobile devices, forcing them to weigh the cost of sharing this information against the possible benefits (Keßler & McKenzie, 2018; Leszczynski, 2017). The rise of artificial intelligence methods and the ubiquity of sensor data have lead many users to conclude that their digital privacy is no longer under their control (Zhang & McKenzie, 2022).

One common motivation for allowing a mobile application access to your location is to share this location with friends, family, acquaintances, or even publicly. A plethora of popular applications exist with this explicit task in mind (e.g., Facebook check-ins, Foursquare's Swarm). The navigation application, Google Maps, one of the most widely used applications on any mobile platform, actively encourages users to share their precise geographic location with friends and family members through their *location-sharing* service (Hill, 2021). All of these platforms realize there is a desire, and a market, for allowing people to share their personal location with one another. While many platforms on the market today offer this service, the existing options built into these platforms fall short.

The vast majority of current services offer users a single choice: either share your precise geographic coordinates with someone or do not share your location at all (as is the case with all the aforementioned platforms). Even applications like Twitter and Instagram only offer limited options for geotagging content, typically restricting to nearby places of interest or one's current city. These limited options do not reflect the wide range of personal, professional, and social relationships that exist. One's level of comfort in sharing one's location with an acquaintance is very different than with one's spouse.

There are also substantial privacy concerns involved in sharing your location with a third-party application. While Google Maps may use your precise location in order to improve traffic prediction or publish real-time popularity values for a business (Google Business Profile Help, 2022; Lau, 2020), and Facebook may use this information to notify you about local events, there is a far more nefarious side to collecting this information (Liccardi & Abdul-Rahman, 2016; Shokri, Theodorakopoulos, Le Boudec, &, Hubaux, 2011). Once your location information is shared with a third-party service, you no longer have control over who has access to the information (Romm, Zhang, Verma, McKenzie, &, Chen, 2021; Thompson & Warzel, 2020). If the primary goal of an application is truly location sharing, the only two parties who should have access to someone's location are the party sharing the information, and the party receiving the information. Accomplishing this in today's data-obsessed culture requires location information to be encrypted by the sender and decrypted by the receiver. This encryption reduces the burden on the party sharing their information as it minimizes the likelihood that a third-party could access the private content, even if the encrypted data are shared publicly.

In this work we present a design pattern and a prototype for a location-sharing application that addresses the aforementioned concerns. We posit that any privacy-preserving location-sharing platform should adhere to three key *design goals*. Specifically, such an application should allow a user to:

1. *Obfuscate their location*. Not only should the user have the option of obfuscating their location once, but they should have the option to obfuscate their location in different ways, depending on the intended recipient of the location information. We refer to these obfuscated locations as *location views*.
2. *Encrypt their location*. Location content should be encrypted in such a way that only those with unique keys can decrypt the information. Furthermore, different location receivers should be given different keys, allowing them to decrypt only the obfuscated location view for which they are the intended recipient.
3. *Share their location*. A user should be able to publish or share a set of obfuscated and encrypted location views once, without having to send unique content to different individuals. Ideally a user should have the option to share these location views publicly without having to manage the process of targeted location sharing.

With these design goals in mind, the objectives of this paper are to demonstrate a design pattern and methodology for achieving the design goals, and to showcase a prototype mobile web platform that employs this design pattern to provide a location-sharing service with real users in mind. The design pattern we outline aims to provide users with control over their location data. We frame this in terms of empowering people to protect their privacy and as a contribution to addressing the *privacy paradox* (Kokolakis, 2017)—the discrepancy between individuals' *stated attitudes* to protect their privacy and their *behaviors* of not actually taking steps to protect their privacy.

2 | BACKGROUND

The number of platforms encouraging people to share their location has grown significantly over the past decade and so too has the body of literature pertaining to this topic. Much of this work discusses privacy concerns through the lenses of passive (Pagani & Malacarne, 2017; Regalia, McKenzie, Gao, &, Janowicz, 2016) or active (Kummer, Ryschka, & Bick, 2018; McKenzie, Janowicz, & Seidl, 2016) location data collection. A considerable literature investigates the reasons why people choose to share their personal location information (Lindqvist, Cranshaw, Wiese, Hong, &, Zimmerman, 2011). While much of this research recognizes that privacy is a concern for most (Kokolakis, 2017; Seidl, Jankowski, Clarke, &, Nara, 2020), they find that for many users the benefits gained from location sharing through services (Budi et al., 2021) or social capital (Ellison, Vitak, Steinfield, Gray, &, Lampe, 2011) outweigh the perceived costs of a loss of privacy. For instance, Alrayes et al. (2020) examined the factors contributing to perception of risk to personal privacy associated with sharing location information on social networking applications. Their findings suggest that the majority of users are privacy pragmatists, willing to share personal data if they experience the benefits.

A common refrain is that, given the degree to which individuals freely divulge private information, share data, and accept terms of service which demand an over-sharing of data, the modern person no longer cares about privacy (Sahota, 2020). Despite this, studies and surveys consistently show that individuals affirm the importance of data privacy. There is a subset of the privacy literature that examines the *privacy paradox*: the discrepancy between users' expressed privacy attitudes and their actual behavior (Barth & de Jong, 2017; Kokolakis, 2017; Norberg & Horne, 2007). When people experience intrusions of their data privacy, they experience a strong negative affective reaction (Budimir, Fontaine, and Roesch, 2021; Durnell, Okabe-Miyamoto, Howell, &, Zizi, 2020). In short, as Coopamootoo and Groß (2017) state, violations of privacy engender fear. Budimir et al. (2021), however, find that the experience of a privacy breach actually can limit the likeliness of individuals to take actions to protect their privacy in the future. Durnell et al. (2020) offer a resolution to this paradox, suggesting that while people care about their privacy, they feel they have no "volitional control." Similarly, Coopamootoo (2018) explains why individuals who fear privacy breaches fail to protect their privacy in terms of a lack of self-efficacy. Other research examining social networking applications concurs, arguing that individuals experience a feeling of a loss of agency or control over their personal data (Chen & Chen, 2015; Rzeszewski & Luczys, 2018). Together, this corpus indicates that users feel disempowered to protect their private data. It follows, then, that a prospective solution is to provide users with the tools to control their privacy, thus granting them more agency, increasing their sense of self-efficacy, and encouraging more proactive privacy protection.

There are a wide range of methods for obfuscating information. The approach most often associated with geographic data involves geomasking.[1] The topic was initially introduced by Armstrong, Rushton, and Zimmerman (1999) for the purpose of preserving the confidentiality of health records but has since been applied in a broad range of fields. Within geomasking, a range of techniques are often employed, from affine transformations to donut masking, and many others (Hampton et al., 2010; Gupta & Rao, 2020; Jiang et al., 2021; Memon et al., 2019). Much of the research on geomasking techniques approaches the topic with a specific domain in mind. For instance, Seidl et al. (2015) investigate the usefulness of different geomasking techniques in household survey data, Almusaylim and Jhanjhi (2020) explore various techniques for preserving the privacy of location-aware

service users, and Tompson et al. (2015) demonstrate the importance of applying geomasking methodologies to crime records. The concept of masking location data has seen broad acceptance by both the academic community and commercial sectors (Kwan, Casas, & Schmitz, 2004; Krumm, 2009). Research has highlighted the tradeoff between the usability of data and preserving the privacy of the individuals sharing their location (Duckham & Kulik, 2005; Olson, Grannis, & Mandl, 2006). While the need for masking is widely acknowledged, previous work has found that a surprising number of academics elect not to mask potentially personal geographic data in publications (Kounadi & Leitner, 2014).

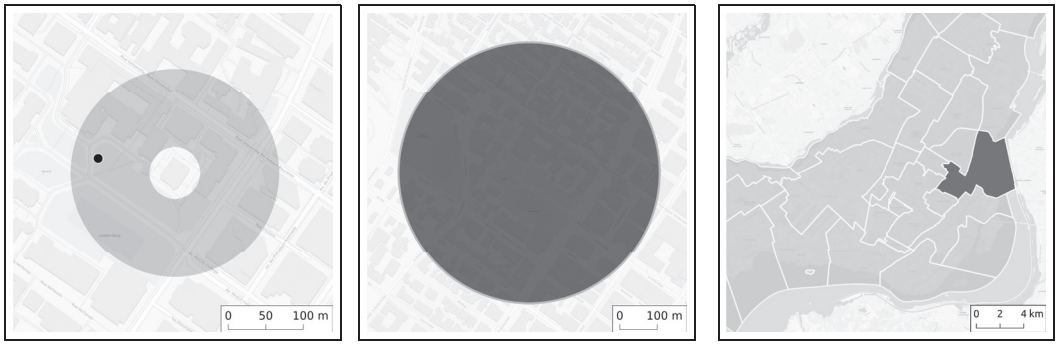
In recent years, new techniques have been developed that leverage unique properties of the data being masked. For instance, Polzin and Kounadi (2021) propose an adaptive technique for residential masking, while Rao et al. (2020) developed an innovative privacy-focused approach to protecting trajectories. Other techniques such as verified neighbor (Richter, 2018) or social trust (Hojati, Farmer, Feick, &, Robertson, 2021) use a modified *k*-anonymity approach. *k*-anonymity is a technique that suggests that by combining a similar set of observations, identifying information about a specific individual, or location, can be obscured, while the data still remain useful. The *k* refers to the user-defined number of similar observations necessary to obfuscate an individual. A number of tools have been developed with the goal of allowing users to mask location data. Swanlund, Schuurman and Brussoni (2020) constructed *MaskMy.XYZ*, a tool for obfuscating geographic data sets through an online web application, and Chen and Poorthuis (2021) developed an R package for identifying (and obfuscating) home locations from mobility data. Drakonakis, Ilia, Ioannidis, &, Polakis (2019) find that if users are given the choice to explicitly select what location data they publish on social networking applications, there is a 95% reduction in attaching their coordinates to their posts. This demonstrates the importance of granting users agency in preserving their privacy.

3 | A DESIGN PATTERN

Given the design goals stated in the introduction, we first propose a design pattern and methodology for any privacy-preserving location-sharing application. While not exclusive, the techniques presented in the following subsections are a suggestive implementation of the scaffolding on which a privacy-preserving application may be constructed. Specifically, we provide an overview of *obfuscation* techniques, a method for *encrypting* location content, and steps for *sharing* one's private location publicly.

3.1 | Obfuscation

One's personal location is an inherently private attribute and one's comfort with sharing this information varies not only by location (e.g., political rally, gay bar) but also by time of day, and with whom the information is being shared. Relationships between individuals vary substantially and so the level of detail with which one's spatiotemporal location is shared should also be permitted to vary. For example, a teenager (likely in consultation with their parents) should have the option to determine how their location is shared. They might share approximate location (say, a circle of radius 500 m) with friends, precise geographic coordinates with family members, and neighborhood-resolution location with the public (in order to facilitate location-specific event invites). The process of varying the accuracy and precision with which one's location is reported is typically referred to as *location obfuscation*. As mentioned in Section 2, this process often relies on an assortment of geomasking techniques. These include random perturbationof location given some distance offset (Figure 1a), representing location as a region (Figure 1b), and selecting from a socially or politically constructed region such as a neighborhood or district (Figure 1c).



(a) Random point within an annulus geometry centered on precise location (Donut Mask)

(b) Circle geometry of specified radius that contains the precise location (Circle Mask)

(c) Neighborhood boundary that contains the precise location (Political Region Mask)

FIGURE 1 A sample of common geomasking techniques. Dark gray regions are the geomasked geometries. Light gray regions shown for reference. Base map by Carto

In building our location-sharing design pattern to achieve *design goal 1*, we allow a user to generate any number of obfuscated location *views*, selecting from a range of geomasking techniques. This means that you can build one view to share with your spouse and a different view to share with your boss. These views are essentially masks through which raw location information is obfuscated. Saving a view simply saves the masking technique and parameters, meaning that any time a set of location views is shared, an individual's current raw geographic coordinates are fed through these masks into the set of user-defined views.

In order to provide the best possible privacy protection for a user, the process of obfuscating one's location should be performed on the client's device with no outside interaction. In other words, an individual's raw geographic coordinates, determined via GNSS or otherwise, should not be sent to a third-party server, geomasked through a potentially vulnerable service, and then returned to the user. The entire process of generating obfuscated location views should take place exclusively on a user's device. For geomasking techniques that involve introducing noise or generating polygons, this is a fairly straightforward process. For techniques that involve intersecting with social or political boundaries, this means that these geometries need to be preloaded on, or downloaded on page-load to, a user's device.

3.1.1 | Temporal obfuscation

When discussing masking, spatial data scientists are typically concerned with obfuscating geographic information, but previous work has demonstrated that the time someone is at a location is also informative (McKenzie & Janowicz, 2015) and knowledge of this exposes one's personal information. It is therefore important to also allow a user to obfuscate their temporal information. While typically not as complex, masking techniques for temporal obfuscation involve rounding to specified temporal units (e.g., hour, date, month, year), reporting only the day (e.g., Tuesday) or reporting a randomized temporal window (e.g., 2 h) in which the actual location event occurred. In the same way that a geomask is chosen by a user and saved as a location view, a temporal mask must also be chosen and added to the location view. While there are numerous options for temporal masking, a key part of this design pattern is that a location-sharing framework should also allow for temporal obfuscation.

3.2 | Encryption

Ensuring that information is shared privately and securely is another essential aspect of a location-sharing platform (*design goal 2*). Having generated a series of location views with various levels of obfuscation, a user then needs to be sure that the view constructed for a target recipient is only accessible by that recipient. Moreover, that recipient should only have access to the intended view, and no others. This task can be accomplished through data encryption. A wide array of options exist for encrypting information that is intended to be shared over a network, many of them suitable for the task at hand. For this design pattern, we recommend employing the Advanced Encryption Standard (AES; Daemen & Rijmen, 1999). The AES is currently a US Government standard for data encryption, used in leading secure communication platforms (e.g., Signal), and has been studied by a range of location researchers (Alrahhal, Ashraf, Abesen, & Arif, 2017; Kachore, Lakshmi, & Nandy, 2015). The benefit of such a standard is that it provides a reasonable tradeoff between speed of encryption/decryption and security. The heart of such an encryption method is a private key (likely represented as a sequence of characters), that is used to encrypt information by one party (the user sharing their location) and decrypt it by another (the intended recipient).

Ideally, keys would be randomly generated to ensure the highest level of security. The longer and more randomized the characters in the key, the more secure. AES keys range in length from 128 to 256 bits. In reality, however, a random sequence of characters may not be the easiest to remember, share, or type into a mobile device, so users should be given the option to construct their own keys. Just like setting a password for any online account, there is a tradeoff between simplicity and security, and that decision lies with the user. For instance, a user may choose to encrypt their non-obfuscated, precise geographic coordinates with a randomly generated 256-bit key, and only encrypt their obfuscated, city-resolution information with the name of their cat. Depending on the level of detail and intended recipient of the location content, a user may decide not to encrypt one of the views at all, with the intention of sharing it publicly.

As was the case with the obfuscation design goal, the entire process of randomly generating or creating a key and encrypting the location views should be performed locally on an individual's mobile client.[2] This is essential to remove any opportunity for raw location information to be intercepted by a third party during data transfer. Only once all the views are encrypted with their respective keys is the user given the option to publish their location content. The sharing of keys is up to the user. Importantly, once a key has been assigned to a location view in such a system, that key will continue to be used to encrypt any further location updates applied to a view. This ensures that the line of communication remains open between the two parties. The user sharing their location has the option to change the key or remove the view entirely for any future location updates, thus cutting off the recipient from any future location information.

3.3 | Sharing

The actual process of sharing the obfuscated and encrypted location views should not be trivialized. As mentioned in the introduction, most current location-sharing applications require someone to share their single, non-obfuscated location view either publicly (e.g., Twitter), with a subset of individuals (e.g., Facebook or Instagram), or directly with an individual (e.g., Google Maps, or any direct messaging service). Each approach has its advantages and disadvantages. Either you publish your location once and share the same amount of detail with everyone, or share it multiple times with different people, depending on who needs it at what time. Unfortunately, for many of the existing companies offering such a service, encrypting the content is not the norm.

Leveraging the obfuscated location views and encryption approaches mentioned above, our location-sharing framework avoids these tradeoffs. Following *design goal 3*, our approach allows a user to publicly share a set of location views while secure in the knowledge that the encryption guarantees that only a certain key can unlock

a particular location view. All other views will remain encrypted and no location content will be shared publicly, unless a user has elected not to encrypt a view.

Since the obfuscation and encryption methods are applied to the location views on the client's mobile device, publication involves wrapping the location views as a single object (e.g., as a JSON array). The object then can be published to a dedicated server, a personal website, or a third-party social media application such as Twitter. Given the potential for a substantial number of nonsensical (to humans) character sequences, one common option for sharing such data would be a quick response (QR) code, or uploading to a server and publishing a static URL that responds to requests with the latest set of location views.

Importantly, the intended recipient(s) of the shared location views must be aware of the data format (e.g., JSON array) through which the location views are shared. If this is known, a recipient can then attempt to decrypt each of the encrypted views in the array until one is successfully decrypted and returns a human or machine-readable location. Attempting to decrypt an encrypted location view with an incorrect key will simply result in another unreadable sequence of characters. This is admittedly a shortcoming of the current publication approach. Future versions of this will include content informing the recipient that the schema of the response is a JSON array of encrypted GeoJSON objects. This would allow a user to design their own decryption script, knowing what to expect should the decryption be successful.

4 | THE PRIVYTO ARCHITECTURE

In the previous sections, we introduced three design goals for a privacy-preserving location-sharing platform as well as a design pattern and methodology for realizing these goals. In this section, we provide an overview of an implementation of the design goals, namely the mobile web application *PrivyTo* (https://privyto.me).

The current prototype of the PrivyTo application runs on a mobile browser and is written using a combination of HTML, CSS, and JavaScript. As outlined in the design pattern, it was important to have all sensitive aspects of the application (obfuscation and encryption) take place exclusively on the client's mobile browser with no external calls over a network. To accomplish this, all the functionality was written in JavaScript and we leveraged a set of JavaScript libraries. The following libraries are downloaded to a user's device when the mobile web application loads.

- *Leaflet* is used to cartographically present a user their current location as well as display previews of the obfuscated location views when selected.
- *Turf.js* is a geospatial analysis library that we use for generating the obfuscated location views. A range of techniques are employed, including point-in-polygon queries, random point generation, polygon creation, and GeoJSON conversion.
- *Crypto-JS* is an encryption library commonly used in web-based applications. We use this library for encrypting and decrypting location views using AES encryption.
- *jQuery* is a commonly used HTML document object manipulation library that allows for fast and robust prototyping.

4.1 | Sharing a location

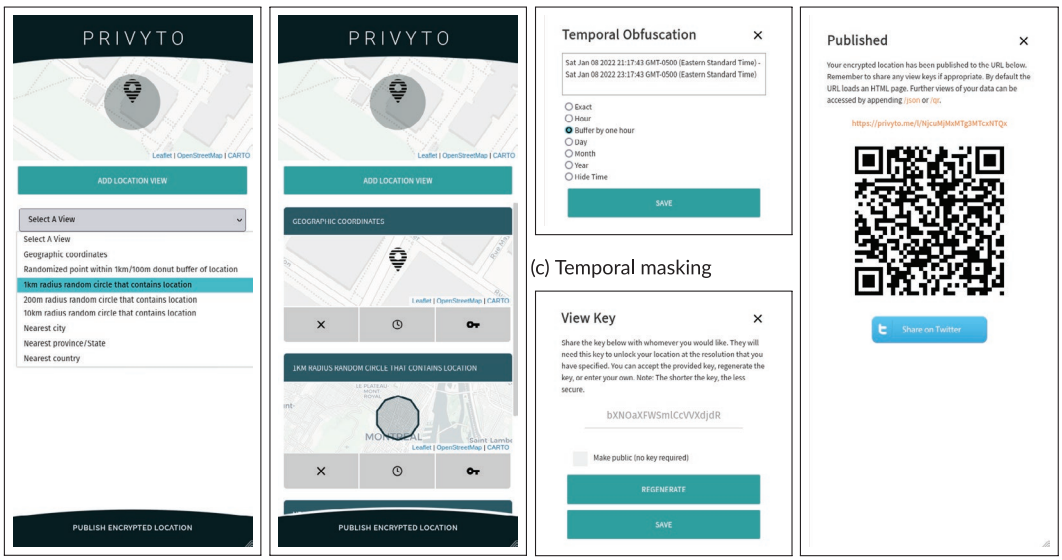
A user begins their interaction with the application by making a mobile browser request to the main PrivyTo website. The user is presented with a login screen where they are given the option to either login to an existing account, create a new account, or share their location once (no login required). By logging in, a user's location object will be published to their account and accessible via a static URL (e.g., https://privyto.me/u/chewbacca). Without

logging in, a user's location object will be published with a unique, randomly generated Base64 22-character identifier that changes each time a user publishes their location (e.g., https://privyto.me/l/NDQuOTg2MTA0NjE3NDE1). Regardless of whether or not a user logs in, the process of creating location views remains the same.

At this point, the user is prompted to share their location by allowing the application, via their mobile browser, access to their current location. In most cases, this location is returned from a GNSS request, but can also be determined via Wi-Fi positioning or cellular trilateration. All of this is handled natively by the browser. Once a location fix has been identified, the user is presented with a screen showing their current location, as well as a circle highlighting the radius of uncertainty. On this screen the user is encouraged to *Add A Location View*. Selecting this option, the user is presented with a series of techniques through which to geomask their location (Figure 2a). Once a location view is selected, the geomask is applied to the user's current location fix and a static map is generated showing a preview of the obfuscated location view. The view is then added to the list of views (Figure 2b). On the device, these location views are stored as a JSON array of GeoJSON objects holding obfuscated locations.[3] Each GeoJSON object also contains a property stating the method used for geomasking as well as the name of the object, if appropriate (e.g., Province of Quebec). At this point, a user can choose to add more views, or select from a series of options to alter an existing view. Specifically, the user can *Delete* the view, *Add a Temporal Mask*, or *View/Edit the Encryption Key*.

In choosing to add a temporal mask, a user is offered a list of temporal masking techniques through which their location publishing time will be obfuscated (Figure 2c). A variety of options are presented with the one shown in the screenshot, randomly generating a two-hour window in which the true time of location publication exists. When the user selects *Save*, the temporal property is added to the GeoJSON representation of the location view as an additional *property* object containing both the temporal value(s) and the type of temporal masking method used.

When a location view is created by the user, a random Base64 22-character (128-bit) key is automatically generated by the platform. By selecting the *key* button associated with the location view, the user can view this key, choose to generate a new unique key, or edit the key to some other sequence of characters (Figure 2d). The minimum length for an AES key is 128 bits and users are encouraged to use long and randomized character keys.



(a) Geomask selection (b) Location Views (c) Temporal masking (d) Encryption key (e) Published

FIGURE 2 Screenshots of the PrivyTo platform demonstrating the workflow of creating location views and publishing an encrypted location object

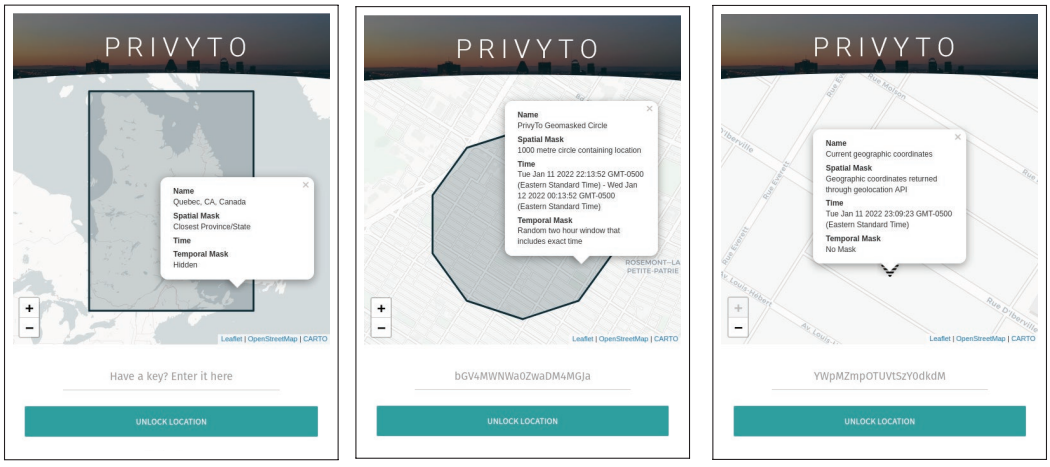
Within this screen, the user can also choose to make the selected location view public, thus indicating that the location view should not be encrypted with the key. At this point, the user should save the key outside of the PrivyTo application in order to share it with its intended recipient.

Once all location views have been generated, temporal masks applied, and keys recorded, the user pushes the *Publish Encrypted Location* button. This executes a process that loops through all location views in the location object and encrypts them with the appropriate key. The encrypted location object is then posted to a web handler on the PrivyTo server along with the session identifier (uniquely generated, or the username if the user is logged in). The encrypted location view is then added to the database. If the location view is associated with a user account, the previous location object is overwritten. A *success* message is returned to the client once the location object is entered into the database. The user is then presented with the public URL for their location object as well as a QR code containing the URL, and an option for sharing this content via social media (Figure 2e).

4.2 | Viewing a location

Once the encrypted location object has been published, a user has a variety of options for sharing their location. First, a user can simply share the URL publicly (e.g., post on a website) or directly with intended recipients. Anyone can visit this URL via a web browser to view the user's location object through an interactive web mapping interface. Remember, however, that only those with keys can unlock encrypted location views. Figure 3 shows the web interface presented to those visiting a user's shared URL. In this scenario, the user has chosen to not encrypt one of their location views, allowing it to be viewed publicly (Figure 3a). On page-load, the application will loop through all location views in the location object to determine if any of them are GeoJSON objects. If one (or more) are identified, these are added to the web map. A user can select the object on the map to view the properties, which include the geospatial masking technique, region name (if appropriate), temporal masking technique, and temporal value.

On this page, a user is also encouraged to enter a key provided by the person sharing their location. After inputting such a key, the application will loop through each of the location views in the location object and attempt



(a) Public view (highly obfuscated location and time)

(b) Private view (less obfuscated location and time) - unlock with key

(c) Private view (no location or time obfuscation) - unlock with key

FIGURE 3 Three views of the same location object. The first view is not encrypted, highly obfuscated and available to the public. The second and third views vary in their obfuscation techniques and require unique decryption keys

```
{
    "data": [
        "{\"type\":\"Feature\",\"bbox\":[-79.765614,44.99803,-57.100331,62.593817],\"properties\":{\"method\":\"Closest Province/
            State\",\"name\":\"Quebec, CA, Canada\",\"time\":{\"mask\":\"Hidden\",\"value\":\"\"}},\"geometry\":{\"type\":\"
            Polygon\",\"coordinates\":[[[-79.765614,44.99803],[-57.100331,44.99803],[-57.100331,62.593817],[-79.765614,62.593817]
        ,[-79.765614,44.99803]]]}}",
        "U2FsdGVkX19u/VUcNfgWNdfCxo+o3WEjAHJBFZKzYrit+VjpEUHbnyCD/gB+Yjq0TOSaYsh3WNLZs/YTlx5N7g/Sskmi87oyjwddHQ/K/
            x5M+rbv5JopUY/9thWeOGtXN4zcnuysgI/b+r4XJf7rfvhQayLlFqMQgOu+2uc7FQlgjvbthLdTLnd+/VWr6JyXi/
            OUJIh8LpTZtbTTN+BhKyzDNFrgp6aqseGfjnGYQli2vUeM+Oi60+PVZs/ZwE1lE/3/kZ+JpwJdVgeP5fXaFXwJRK5/pvV45H/x1MPvo4lTRys9fKFdzqz
        mkTm7pUrgjtUlLzs49B8wF1rzeTr1xXsupkeMtHsQ8tzHFThmwLTyggLqMGvAbmwlvdWJosr2s3JfcJPU31WT71C3GGIORXjK1iVg8HVHsKghdo2hUWLuaMQf
        GSEGAnb5tXTAzxfz+LtfBaf5nVU9yAGAfRaHGc426w5yIIxqQ+2Mh4nvQTVZQtUgHw6dl0ewYjNadPdftfL7M9LbLxY3z3qf2TwN4jeJIFWFGgPst5
            DBRmkoPMmcjU9ihbEFIbbc3WW6ZIr9oxeWg3vq8ViU22RRfE1zSUES3+huPTz/
            saXiQKMYFCT3RmDtxnukcyrON7mEP0qyyIseHmMtMUtsmeZixqgXottguMiWu24nIbp+M6SrxA7GbRkE2Vu6sd4EOM7tZhhlOtX5eJk/
            FlqEKOjt5QW4rIJKm7td/BywCTj4sdaU0XjMzdiovPauOZ7AeGX+yapg/tOAXN85OPwZ52MggtbJMcX/
            d+PYTIruZSMnEzy0213+Tyb7S65k1HBvkCe35TijzNH3dlEriaZVNn7QivH9kV3IftwqBv5BWJHbfltjvuM64OC1A3LlAf2S/2NM55WU",
        "U2FsdGVkX1+SwYh2P1d/cYHRIKPqKONnhGclqIm0gilExPH24SHEQ2yuz7+osSS3bkNpcWn2a5Jfmxcrjwui49IUKf3SzAnJ1nCdfluul/8GNVLPH2jsDtJ4
        GVgHRqsMRqoQugLObFjQYEHZOxXwNE49QpVdWn7yp6u01J8Yn1XxmMddcMeAbhUYeX7Nw4aD1z/
            opQXZSyjwOGRpHbBn789JN3F3rZdoQXksvG0E6GxnE1GXKFFrmFRzYA7fyxZz3BSjUgc9EUCm/ZAaqMGuNSMmNVmJb3RileUbcf6Y7ggwh6DUeF56ZVBa
        +Kinw56ujewvKye65gyN/78fygX7J64pYyNm8yhkrTeYMd7lCoDspsDdzgIsHygL+cfCUjM7H2nEscIdq9ojIe7UjKIUvFpzSBD15wUi0kKedafWqnXAldFvi
            UxDGse1LL9A6/GxGr/I9XDlvzzX9zQESsJzxq=="
    ],
    "meta": {
        "code": 200,
        "response": "Success."
    }
}
```


FIGURE 4 JSON response from the server containing the location object. This specific object contains an array of three location views (same as Figure 3). The two highlighted in red are encrypted with unique keys (precise geographic coordinates and circle obfuscation), while the location view highlighted in green (province bounding box) is not encrypted and intended for public consumption. HTTP response status codes are provided in the *meta* property

to decrypt them with the key. If the result of the decryption method is a valid GeoJSON object, the newly discovered geographic entity is added to the map, replacing any previous items. As shown in Figures 3b,c, different geographic objects are presented to the user depending on the key that they provide.

In addition to the interactive platform for viewing a user's location object, a user (or machine) can view the raw encrypted location object in JSON format by appending `/json` to the URL (Figure 4). This is useful to those individuals interested in storing the location, using the location in a third-party application, or embedding the location object in their personal website. Similarly, a user can append `/qr` to view a quick response code representation of the location object. This is primarily to enable accessible sharing of the raw location data.

4.3 | Location storage

On a user's device, any time that a location view is created or updated, the array of location views is updated in the *localStorage* property of the *Window* interface accessible within all modern mobile browsers (https://html.spec.whatwg.org/multipage/webstorage.html#the-localstorage-attribute). The use of *localStorage* keeps the unencrypted location views on the device, so that when a user returns to the PrivyTo platform, their saved geomasks are reapplied to their updated location fix, allowing them to simply publish the location object rather than being forced to redo the entire process of creating location views, keys, temporal masks, and so on.

When an encrypted location object is published from the web-based mobile application, it is received by the web handler on the server and added to one of two tables. If a user has been authenticated (via login), their encrypted location object is updated in the `user_location` table. This overwrites any existing location object. In this prototype version of the application it was decided, for privacy reasons, that the server should not store a history of a user's location, instead only storing the most recent location object. If a user is not authenticated (i.e., not logged in), their encrypted location object is added to the `guest_location` table using the auto-generated identifier as a unique ID in the table. A third table (`users`) stores authenticated user details used for creating accounts and validating logins. All connections between the client's mobile web browser and the PrivyTo.me server are encrypted using SHA-256 with RSA Encryption.

5 | DISCUSSION

In the previous two sections we outlined a design pattern for a location-sharing application and showcased a functioning prototype that implements the design pattern. These are presented in response to design goals that we identified as being important aspects to any privacy-preservation platform in operation today. While not exhaustive, these three design goals present the foundation for a system that has the user's interest at heart and does not come at a cost of sharing one's privacy location information with a third party.

A large body of work has demonstrated that while commercial companies may offer free services through which to share content, their desire to leverage personal location data for advertising revenue is at odds with their promise of privacy (Newman, 2021). Concern over the use of private data is at an all-time high, so the tools that we use to share our personal information should reflect this. Our privacy-preserving platform empowers users to protect their geoprivacy. It is our hope that in doing so, individuals who would otherwise not take actions to protect their location data begin to do so as they are granted a sense of agency and control. This work is also intended to spur further discussion on the topic and encourage further development within the location privacy community.

5.1 | Limitations

One of the difficulties with geomasking location information is that the level of privacy varies depending on context. For instance, a random 200-meter perturbation of one's location in the downtown core of a major metropolis provides far more privacy preservation than that same technique applied in a rural community. The approach that we propose, of constructing location views through which one's location is obfuscated means that the level of privacy actually varies depending on where the location view is used. The same could be said for the temporal obfuscation methods. Temporally masking one's location by 2 hours at 5 p.m. on a Friday preserves one's privacy to a greater degree than at 4 a.m. on a Tuesday. In the first case, there are plenty of possible activities that one could be engaged in between 4 and 6 p.m. on a Friday. There are far fewer options between 3 and 5 a.m. on a Tuesday. While our method of giving users the option of picking their own geomasking technique is a significant step in the right direction, we will explore context-aware approaches (e.g., Cassa, Grannis, Overhage, &, Mandl, 2006) in future iterations of this project.

An issue with many encryption techniques that involve sharing keys is that while the key can be changed before sharing future encrypted content, previously shared content will continue to be accessible by the key holder. This is true for our current design approach as well. Previously encrypted location views will always be accessible to a user who was given the key used to encrypt the location, and there is nothing that a person sharing the data can do to remove their access to previously published location objects.[4]

Lastly, while obfuscation and encryption take place on a user's mobile device, their location is technically still exposed to the base map tile server. Storing high-resolution base map tiles for the entire globe is not feasible for a mobile web application, so the PrivyTo platform requests map tiles from a third-party (Carto) tile server. In order to provide a base map to the application user, code in the web mapping frame work (Leaflet) sends a request to the tile server that includes the bounding box of the map window on the device. This is generated from the user's precise location and current zoom level. While the company running the tile server has no information on the actual user requesting the tiles, the server does receive a request from their IP address as well as the rough location (in order to return the appropriate subset of tiles). This information could be used to identify a user should a malicious actor gain access to the tile server logs. To mitigate this issue, future versions of the PrivyTo application will offer users the option to disable base map tile requests.

5.2 | Future work

There are a number of future directions in which we would like to take this work. First, we would like to increase the number of geomasking techniques offered for location obfuscation. The set provided in the prototype is primarily meant to demonstrate the capabilities of such a platform. Future steps will involve allowing for custom geomasking algorithms and the addition of user-controlled weights or parameters.

While further discussion is necessary on best practices, we intend to explore options for sharing user trajectories, place instances (e.g., Mel's Diner), and allowing for a history of location objects to be stored and shared. There are further privacy issues to be considered with each of these ideas and our future work will explore them from both a technical and theoretical perspective.

With regard to the prototype application, we are currently developing native Android and iOS applications to allow users to share their locations at semi-regular intervals, run the applications in the background, and generally encourage a better user experience. Our next steps in this domain are to push further into the native Android operating system and explore options for embedding such a design pattern into the base location-sharing functionality of the operating system itself. For instance, instead of a user only being able to use *Facebook Event Notifications* by sharing their precise location, the user could instead have greater control over the resolution of location information they provide. Basic location-spoofing applications already exist for the Android platform, but few offer such a range of obfuscation techniques.

5.3 | Conclusions

Location privacy has long been a popular research topic. Recent advances in ubiquitous sensor technology have spurred a renewed interest in the topic. Social media platforms and digital service providers have become so pervasive that we rarely think twice about sharing location content through these platforms. In an effort to empower users with the option to share personal data privately, we have developed a set of design goals, a design pattern, and a prototype application for securely and privately sharing location content. Our approach leverages geomasking and location-obfuscation techniques, encryption technologies, and a novel perspective on sharing. In presenting our approach, this work is intended to showcase the issues with existing location-sharing applications and offer a solution that puts the user back in control of their personal location information.

ENDNOTES

[1] Referred to as *spatial-temporal cloaking* in some domains.

[2] Such a system could be implemented through any browser (mobile or other). We refer to mobile throughout this article as this is likely to be the most commonly used platform.

[3] Given the complexity of some geometries, political boundaries such as provinces or states are simply stored using their name and bounding box.

[4] The data or link to the data can be removed from the server, but if the location views themselves have been downloaded, access cannot be removed.

REFERENCES

Almusaylim, Z. A., & Jhanjhi, N. (2020). Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing. *Wireless Personal Communications*, *111*, 541–564. https://doi.org/10.1007/s11277-019-06872-3

Alrahhal, M. S., Ashraf, M. U., Abesen, A., & Arif, S. (2017). AES-route server model for location based services in road networks. *International Journal of Advanced Computer Science and Applications*, *8*, 361–368.

Alrayes, F. S., Abdelmoty, A. I., El-Geresy, W., & Theodorakopoulos, G. (2020). Modelling perceived risks to personal privacy from location disclosure on online social networks. *International Journal of Geographical Information Science*, *34*, 150–176. https://doi.org/10.1080/13658816.2019.1654109

Armstrong, M. P., Rushton, G., & Zimmerman, D. L. (1999). Geographically masking health data to preserve confidentiality. *Statistics in Medicine*, *18*, 497–525.

Barth, S., & de Jong, M. D. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior, a systematic literature review. *Telematics and Informatics*, *34*, 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bohn, J., Coroamă, V., Langheinrich, M., Mattern, F., & Rohs, M. (2005). Social, economic, and ethical implications of ambient intelligence and ubiquitous computing. In W. Weber, J. Rabaey, & E. Aarts (Eds.), *Ambient intelligence* (pp. 5–29). Berlin, Germany: Springer.

Budi, N. F. A., Adnan, H. R., Firmansyah, F., Hidayanto, A. N., Kurnia, S., & Purwandari, B. (2021). Why do people want to use location-based application for emergency situations? The extension of UTAUT perspectives. *Technology in Society*, *65*, 101480.

Budimir, S., Fontaine, J. R., & Roesch, E. B. (2021). Emotional experiences of cybersecurity breach victims. *Cyberpsychology, Behavior, and Social Networking*, *24*, 612–616. https://doi.org/10.1089/cyber.2020.0525

Cassa, C. A., Grannis, S. J., Overhage, J. M., & Mandl, K. D. (2006). A context-sensitive approach to anonymizing spatial surveillance data: Impact on outbreak detection. *Journal of the American Medical Informatics Association*, *13*, 160–165. https://doi.org/10.1197/jamia.M1920

Chen, H.-T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*, 13–19. https://doi.org/10.1089/cyber.2014.0456

Chen, Q., & Poorthuis, A. (2021). Identifying home locations in human mobility data: An open-source r package for comparison and reproducibility. *International Journal of Geographical Information Science*, *35*, 1425–1448. https://doi.org/10.1080/13658816.2021.1887489

Coopamootoo, K. P. (2018). Work in progress: Fearful users' privacy intentions, an empirical investigation. In *Proceedings of the Seventh Workshop on Socio-Technical Aspects in Security and Trust*, Orlando, FL (pp. 82–89). New York, NY: ACM.

Coopamootoo, K. P., & Groß, T. (2017). Why privacy Is all but forgotten: An empirical study of privacy and sharing attitude. *Proceedings on Privacy Enhancing Technologies*, *2017*, 97–118. https://doi.org/10.1515/popets-2017-0040

Daemen, J., & Rijmen, V. (1999). *AES proposal: Rijndael*. Unpublished document.

Drakonakis, K., Ilia, P., Ioannidis, S., & Polakis, J. (2019). Please forget where I was last summer: The privacy risks of public location (meta)data. In *Proceedings of the 2019 Network and Distributed Systems Security Symposium*. San Diego, CA. (pp. 1–15).

Duckham, M., & Kulik, L. (2005). A formal model of obfuscation and negotiation for location privacy. In H. W. Gellersen, R. Want, & A. Schmidt (Eds.), *Pervasive computing: Pervasive Computing 2005* (Lecture Notes in Computer Science, Vol. *3468*, pp. 152–170). Berlin, Germany: Springer.

Durnell, E., Okabe-Miyamoto, K., Howell, R. T., & Zizi, M. (2020). Online privacy breaches, offline consequences: Construction and validation of the concerns with the protection of informational privacy scale. *International Journal of Human-Computer Interaction*, *36*, 1834–1848. https://doi.org/10.1080/10447318.2020.1794626

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte, & L. Reinecke (Eds.), *Privacy online* (pp. 19–32). Berlin, Germany: Springer.

Gambs, S. (2018). Privacy and ethical challenges in big data. In N. Zincir-Heywood, G. Bonfante, M. Debbabi, & J. Garcia-Alfaro (Eds.), *Foundations and practice of security: FPS 2018* (Lecture Notes in Computer Science, Vol. *11358*, pp. 17–26). Cham, Switzerland: Springer.

Google Business Profile Help. (2022). *Popular times, wait times, and visit duration*. Retrieved from https://support.google.com/business/answer/6263531?hl=en

Gupta, R., & Rao, U. P. (2020). Preserving location privacy using three layer RDV masking in geocoded published discrete point data. *World Wide Web*, *23*, 175–206. https://doi.org/10.1007/s11280-019-00716-7

Hampton, K. H., Fitch, M. K., Allshouse, W. B., Doherty, I. A., Gesink, D. C., Leone, P. A., & Miller, W. C. (2010). Mapping health data: Improved privacy protection with donut method geomasking. *American Journal of Epidemiology*, *172*, 1062–1069. https://doi.org/10.1093/aje/kwq248

Hill, S. (2021). *How to share your location on an iPhone or Android*. Retrieved from https://www.wired.com/story/how-toshare-your-location-android-ios/

Hojati, M., Farmer, C., Feick, R., & Robertson, C. (2021). Decentralized geoprivacy: leveraging social trust on the distributed web. *International Journal of Geographical Information Science*, *35*(12), 2540–2566. https://doi.org/10.1080/13658816.2021.1931236

Jiang, H., Li, J., Zhao, P., Zeng, F., Xiao, Z., & Iyengar, A. (2021). Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys*, *54*, 1–36.

Kachore, V. A., Lakshmi, J., & Nandy, S. (2015). Location obfuscation for location data privacy. *Proceedings of the 2015 IEEE World Congress on Services*, New York, NY (pp. 213–220). Piscataway, NJ: IEEE.

Keßler, C., & McKenzie, G. (2018). A geoprivacy manifesto. *Transactions in GIS*, *22*, 3–19. https://doi.org/10.1111/tgis.12305

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kounadi, O., & Leitner, M. (2014). Why does geoprivacy matter? The scientific publication of confidential data presented on maps. *Journal of Empirical Research on Human Research Ethics*, *9*, 34–45. https://doi.org/10.1177/1556264614544103

Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing*, *13*, 391–399. https://doi.org/10.1007/s00779-008-0212-5

Kummer, T.-F., Ryschka, S., & Bick, M. (2018). Why do we share where we are? The influence of situational factors on the conditional value of check-in services. *Decision Support Systems*, *115*, 1–12. https://doi.org/10.1016/j.dss.2018.08.012

Kwan, M.-P., Casas, I., & Schmitz, B. (2004). Protection of geoprivacy and accuracy of spatial information: How effective are geographical masks? *Cartographica*, *39*, 15–28. https://doi.org/10.3138/X204-4223-57MK-8273

Lau, J. (2020). *Google Maps 101: How AI helps predict traffic and determine routes*. Retrieved from https://blog.google/products/maps/google-maps-101-how-ai-helps-predict-traffic-and-determine-routes

Leszczynski, A. (2017). Geoprivacy. In R. Kitchin, T. P. Lauriault, & M. W. Wilson (Eds.), *Understanding spatial media* (pp. 235–244). Thousand Oaks, CA: SAGE Publications.

Liccardi, I., & Abdul-Rahman, A. (2016). I know where you live: Inferring details of people's lives by visualizing publicly shared location data. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, San Jose, CA (pp. 1–12). New York, NY: ACM.

Lindqvist, J., Cranshaw, J., Wiese, J., Hong, J., & Zimmerman, J. (2011). I'm the mayor of my house: Examining why people use Foursquare, a social-driven location sharing application. In *Proceedings of the 2011 SIGCHI Conference on human Factors in Computing Systems*, Vancouver, BC, Canada (pp. 2409–2418). New York, NY: ACM.

McKenzie, G., & Janowicz, K. (2015). Where is also about time: A location-distortion model to improve reverse geocoding using behavior-driven temporal semantic signatures. *Computers, Environment and Urban Systems*, *54*, 1–13. https://doi.org/10.1016/j.compenvurbsys.2015.05.003

McKenzie, G., Janowicz, K., & Seidl, D. (2016). Geo-privacy beyond coordinates. In T. Sarjakoski, M. Santos, & L. Sarjakoski (Eds.), *Geospatial data in a changing world* (pp. 157–175). Cham, Switzerland: Springer.

Memon, I., Mirza, H. T., Arain, Q. A., & Memon, H. (2019). Multiple mix zones de-correlation trajectory privacy model for road network. *Telecommunication Systems*, *70*, 557–582. https://doi.org/10.1007/s11235-019-00551-1

Newman, L. H. (2021). *WhatsApp has shared your data with Facebook for years, actually*. Retrieved from https://www.wired.com/story/whatsapp-facebook-data-share-notification

Norberg, P. A., & Horne, D. R. (2007). Privacy attitudes and privacy-related behavior: Privacy attitudes and privacy-related behavior. *Psychology & Marketing*, *24*, 829–847. https://doi.org/10.1002/mar.20186

Olson, K. L., Grannis, S. J., & Mandl, K. D. (2006). Privacy protection versus cluster detection in spatial epidemiology. *American Journal of Public Health*, *96*, 2002–2008. https://doi.org/10.2105/AJPH.2005.069526

Pagani, M., & Malacarne, G. (2017). Experiential engagement and active vs. passive behavior in mobile location-based social networks: The moderating role of privacy. *Journal of Interactive Marketing*, *37*, 133–148. https://doi.org/10.1016/j.intmar.2016.10.001

Polzin, F., & Kounadi, O. (2021). Adaptive Voronoi masking: A method to protect confidential discrete spatial data. In K. Janowicz, & J. A. Verstegen (Eds.), *11th International Conference on Geographic Information Science (GIScience 2021): Part II* (Leibniz International Proceedings in Informatics, Vol. *208*, pp. 1:1–1:17). Dagstuhl, Germany: Schloss Dagstuhl–LeibnizZentrum für Informatik.

Rao, J., Gao, S., Kang, Y., & Huang, Q. (2020). LSTM-TrajGAN: A deep learning approach to trajectory privacy protection. In K. Janowicz, & J. A. Verstegen (Eds.), *11th International Conference on Geographic Information Science (GIScience 2021): Part I (Leibniz International Proceedings in Informatics* (Vol. *177*, pp. 12:1–12:17). Dagstuhl, Germany: Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

Regalia, B., McKenzie, G., Gao, S., & Janowicz, K. (2016). Crowdsensing smart ambient environments and services. *Transactions in GIS*, *20*, 382–398. https://doi.org/10.1111/tgis.12233

Richter, W. (2018). The verified neighbor approach to geoprivacy: An improved method for geographic masking. *Journal of Exposure Science & Environmental Epidemiology*, *28*, 109–118. https://doi.org/10.1038/jes.2017.17

Romm, D., Zhang, H., Verma, P., McKenzie, G., & Chen, E. (2021). "Data horror": Mapping (spatial) data privacy violations onto a cognitive account of horror. In *Proceedings of the 2021 Spatial Data Science Symposium*, Santa Barbara, CA (pp. 1–6). Santa Barbara, CA: University of California Santa Barbara: Center for Spatial Studies.

Rzeszewski, M., & Luczys, P. (2018). Care, indifference and anxiety: Attitudes toward location data in everyday life. *ISPRS International Journal of Geo-Information*, *7*, 383. https://doi.org/10.3390/ijgi7100383

Sahota, N. (2020). *Privacy is dead and most people really don't care*. Retrieved from https://www.forbes.com/sites/neilsahota/2020/10/14/privacy-is-dead-and-most-people-really-dont-care/?sh=53d8695c7b73

Seidl, D. E., Jankowski, P., Clarke, K. C., & Nara, A. (2020). Please enter your home location: Geoprivacy attitudes and personal location masking strategies of internet users. *Annals of the American Association of Geographers*, *110*, 586–605. https://doi.org/10.1080/24694452.2019.1654843

Seidl, D. E., Paulus, G., Jankowski, P., & Regenfelder, M. (2015). Spatial obfuscation methods for privacy protection of household-level data. *Applied Geography*, *63*, 253–263. https://doi.org/10.1016/j.apgeog.2015.07.001

Shokri, R., Theodorakopoulos, G., Le Boudec, J.-Y., & Hubaux, J.-P. (2011). Quantifying location privacy. In *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, Oakland, CA (pp. 247–262). Piscataway, NJ: IEEE.

Swanlund, D., Schuurman, N., & Brussoni, M. (2020). MaskMy.XYZ: An easy-to-use tool for protecting geoprivacy using geographic masks. *Transactions in GIS*, *24*, 390–401. https://doi.org/10.1111/tgis.12606

Thompson, S. A., & Warzel, C. (2020). *Twelve million phones, one dataset, zero privacy*. Retrieved from https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

Tompson, L., Johnson, S., Ashby, M., Perkins, C., & Edwards, P. (2015). UK open source crime data: Accuracy and possibilities for research. *Cartography and Geographic Information Science*, *42*, 97–111. https://doi.org/10.1080/15230406.2014.972456

Warzel, C., & Thompson, S. A. (2021). *They stormed the Capitol: Their apps tracked them*. Retrieved from https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html

Weber, R. H. (2010). Internet of things-new security and privacy challenges. *Computer Law & Security Review*, *26*, 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

Zhang, H., & McKenzie, G. (2022). Rehumanize geoprivacy: From disclosure control to human perception. *GeoJournal*, https://doi.org/10.1007/s10708-022-10598-41-20

How to cite this article: McKenzie, G., Romm, D., Zhang, H., & Brunila, M. (2022). PrivyTo: A privacy-preserving location-sharing platform. *Transactions in GIS*, *00*, 1–15. https://doi.org/10.1111/tgis.12924