安全
anZen

November 6, 2009

Federal Trade Commission
Office of the Secretary, Room H-135 (Annex P)
600 Pennsylvania Avenue NW
Washington, DC 20580

Anzen Consulting Inc.
38 Elm Street, Suite 3410
Toronto, ON, Canada
M5G 2K5

Re: Privacy Roundtables – Comment, Project No. P095416

Anzen Consulting Inc. ("Anzen") is an independent consulting firm specializing in information privacy. Anzen has researched and advised on emerging technologies such as geospatial applications, health information technology, data mining/linking, online behavioral advertising, and online marketing programs. Anzen's team is comprised of technical and security experts, lawyers, informatics specialists, and former privacy officers, who review technology from a technical, legal, and business perspective.

We would like to thank you for the opportunity to comment on the privacy risks, concerns, and benefits that arise from the collection, sharing, and use of consumer information. Our comments apply our international research on privacy regulatory, self-regulatory, and best practices to **location-based applications**. Commercial location-based applications utilize a user's location (based on the global positioning of the user's mobile device, the location entered by the user, or information accessed through satellites or other global information systems) to provide the user with services and information through his or her mobile device. The services and information may include, for example, enabling the user to locate a business (e.g. restaurant) or service (e.g. bank machine) near his or her location, or to gain access to information about his or her location, such as transportation routes, weather, or tourist attractions. Recently, information technology companies have integrated location-based and social networking applications (e.g. Foursquare, Latitude). These applications enable users to locate other people registered to use the application(s) through the user's mobile device.

Our comments on this topic are organized into four sections. In **Section 1**, we provide an overview of Anzen and our privacy experience with emerging technologies. In **Section 2**, Anzen summarizes the types of location-based applications upon which our comments are based and defines information privacy as it relates to these applications. In **Section 3**, we discuss the privacy risks inherent to location-based applications and the privacy regulatory and best practices emerging to mitigate these risks. Our comments in Section 3 are organized as follows:

- **Privacy Legal Framework:** Anzen explores privacy-legal regimes that are evolving to address "location" as an identifiable data element by discussing recent developments in Europe and Canada. In doing so, Anzen discusses the concepts of spatial and information privacy, the gaps in existing legislation, and our recommendations to address privacy issues concerning location-based applications through regulation.
- **Informed Consent:** Anzen discusses the mechanisms in place to inform users about how their location and related information is collected, used, inferred, and disclosed and the level of information that is required to ensure users' consent is informed and knowledgeable.

- **Aggregation of Location-Based Information:** Anzen explores the risks associated with the aggregation of location-based information. The secondary uses we discuss include websites, which harvest information from location-based applications and sites to create new applications and services, and private firms, which mine geospatial information and link it with existing databases to understand consumer interests and market products and services. Anzen discusses the risks to sensitive groups, who wish to keep their locations concealed, and to consumers, who have little control over the use of their information for secondary purposes. Further, Anzen discusses the difficulty in regulating secondary uses and the regimes that are being adopted to address this issue.

In the final section (**Section 4**), we have listed biographies for all the members of the Anzen team, including the Anzen privacy consultants and lawyers who have contributed to our comments, Michelle Gordon (author), Jordan Prokopy (author), and Megan Brister (editor).

Thank you again for this opportunity to comment on the privacy aspects of location-based applications. We hope that our comments serve to inform the Federal Trade Commission's work in this area.

Sincerely,

Miyo Yamashita, PhD

安全
anZen

1 About Anzen

Anzen Consulting Inc. ("Anzen") is an independent consulting firm specializing in information privacy. Anzen provides solutions for clients in a variety of areas, regardless of geography or industry sector. We have developed our areas of expertise by helping clients with problems that involve the management of personal information, including marketing, advertising, employee privacy, health, and new and emerging technologies, such as geospatial applications, among others.

We are experts in conducting privacy impact assessments, privacy gap assessments, and privacy legal analyses. We also provide our clients with privacy advisory services in the areas of privacy risk management, privacy crisis management, privacy policy development and implementation, staff privacy education and training, and the application of privacy laws and "best practices" relating to the collection, use, and disclosure of sensitive personal information, such as social insurance numbers, household incomes, and personal health information.

Emerging technologies, such as cloud computing, geospatial applications, social media and networking, and location-based applications pose potentially significant risks to individual privacy. Anzen's multi-disciplinary team of lawyers, technical experts, informatics specialists and former privacy officers review technologies from a legal, technical, and business perspective. Anzen assists private companies, regulators, and trade organizations by researching the privacy implications of new and emerging technologies and by developing policy positions around the use of these technologies.

We believe it is important to contribute to the privacy discussion concerning emerging technology, including location-based applications. To this end, we are grateful for the opportunity to submit the enclosed comments to the Federal Trade Commission and to participate in the dialogue in this important area.

2 Collection, Use, and Disclosure of Information via Location-Based Applications

Location-based applications connect information with a specific user's location to deliver services to the user. Some of these applications include online mapping interfaces or "geo-browsers", such a Google Streetview or Microsoft's Bing Maps, which enable a user to browse and identify geographical locations (e.g. streets of New York) and geospatial information (e.g. user's coordinates), and overlay it with additional information. Other commercial location-based applications use the global positioning of an individual's mobile device or an address entered by the user to identify his or her location. Once the user's location is known, the company can provide services relevant to this location, such as directions, transportation options, or nearby businesses or services. The company relies on its own and/or third party geospatial information to provide users information about the venues and services around them. Companies may also identify a user's location using a global positioning device installed in, for example, the individual's car. Some companies monitor their mobile sales force in this way.

Recently, location-based applications have converged with social networking and media technology to enable users to not only access information about *what* is around them, but also about *who* is around them. For example, Google Latitude is a feature of Google Maps that enables individuals with Gmail accounts to share their locations with "friends". Friends can see the user's screen name, location, and the time the individual was at the location on Google Maps by using his or her mobile device or iGoogle. Individuals sign up for Latitude by downloading the application from their mobile devices. In order for the user to share his or her location, he or she must invite a friend to view his or her location. The friend may: 1) accept the request (and, therefore, see the user's location) and also share his or her location; 2) accept the request, but not share his or her location; or 3) reject the request altogether. Users can also block others from contacting them with invitations.

Foursquare is another example of the convergence of location-based and social networking technology. However, Foursquare also incorporates elements of gaming and social competition. Foursquare is based on a system of "checking-in" with a mobile phone from bars, restaurants, art galleries, and any kind of nightspot, with a brief message about where the user is and what he or she is doing. Foursquare will then register this information and alert the user's friends to his or her current whereabouts and activities. The system acts as a competitive game by awarding points to players depending on how often they go out and which places they visit (e.g. users receive one point for checking in and five points if the user is new to the location).

The companies offering location-based applications generally collect geospatial information (i.e. information about a location), as well as personal information, such as phone number and preferences (e.g. preferred settings, social networking account information) from users directly, as well as through satellites and global positioning systems.[1]

In the case of Latitude, for example, users agree to the collection and use of their information for the purposes of receiving location-based services from the companies by downloading, installing, and using the applications.[2] Companies may also use the information to monitor the success of an application, make improvements, or manage inquiries. This information may also be linked with other information already collected about users in order to better understand user preferences.

---

[1] See Brightkite Privacy Policy at: http://apps.brightkite.com/pages/bk_privacy_policy.html.

[2] See Google Mobile Help > Privacy > Location Privacy: http://google.com/support/mobile/bin/answer.py?hl=en&answer=136654.

Finally, companies do not routinely disclose geospatial information. For example, Google's privacy information on Latitude states that it does not share a user's location with third parties without explicit permission.[3] Brightkite, an application similar to Foursquare, states in its Privacy Policy that non-identifying information is provided to third parties for industry analysis, demographic profiling, and to deliver targeted advertising about other products and services.[4]

[3] See Google Mobile Help > Privacy > Location Privacy: http://google.com/support/mobile/bin/answer.py?hl=en&answer=136654.

[4] See Brightkite Privacy Policy at: http://apps.brightkite.com/pages/bk_privacy_policy.html.

3 Anzen's Comments on Location-Based Applications

3.1 Privacy Legal Framework

In this section, Anzen discusses the legal frameworks being developed in various jurisdictions in response to the growing importance of "location data" as a privacy issue. First, this section addresses the current legal framework in the United States. Second, Anzen outlines recent developments in Europe and Canada in order to understand how other jurisdictions have responded – or have failed to respond – to this emerging technology. Finally, this section discusses the lack of specific regulation in this emerging area and makes recommendations as to how these issues may be addressed through regulation.

3.1.1 US Framework

In the US, lawmakers have given some attention to developing a legal framework for location privacy through enacted and proposed federal legislation.

The *Wireless Communications & Public Safety Act of 1999*[5] (aka the 911 Act) specifically addressed a common fear that wireless (i.e. cell phone) customers would be foregoing their right to location privacy because of government-imposed mandatory locating tracking devices. The purpose of the 911 Act is to enhance public safety by encouraging and facilitating the prompt deployment of a nationwide, seamless communications infrastructure for emergency services that includes wireless communications. Practically speaking, the Federal Communications Commission (FCC) began implementing the Act by adopting rules creating a special method for processing 911 calls. For example, all wireless phones manufactured after February 2000 had to allow 911 calls to be routed to any available provider rather than to the customer's preferred service provider. The 911 Act also sought to specifically identify a mobile caller's location, which required new technology.[6]

The 911 Act specifically defines "location" as one of the sensitive categories of data that require protection by telecommunications carriers. Specifically, the Act recognizes the right to privacy of location information by classifying location information as customer proprietary network information subject to section 222 of the *Communications Act of 1934* (47 U.S.C. 222), thereby forbidding carriers from accessing, using, or disclosing wireless location information "without the express prior authorization of the customer".

Although the 911 Act was clearly intended to protect consumers and their information, a US appellate court found, soon after its enactment, that the privacy protections set out in the Act had unconstitutionally limited the First Amendment rights of telecom companies. In *U.S. West v. FCC*, the Court of Appeals for the Tenth Circuit invalidated those provisions of the Act which granted consumers default protection of their personal information. The Court held that Congress must offer a compelling state interest before protecting a privacy interest.

In 2001, Congress introduced the *Location Privacy Protection Act*.[7] In reaction to the decision in *U.S. West v. FCC*, this Act offers the compelling state interest of public safety, as well as the privacy interest of protection of location information. Although this legislation was never enacted, its provisions demonstrate a broad, technology-neutral approach to location privacy issues. The Act defines "location information" as non-public information that can be misused to commit fraud, to harass consumers with unwanted messages, to draw embarrassing or

[5] Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286.

[6] Electronic Privacy Information Center: http://epic.org/privacy/location/jwhitelocationprivacy.pdf.

[7] The Act is available at: http://thomas.loc.gov/cgi-bin/query/z?c107:S.1164:.

inaccurate references about them, or to discriminate against them. The Act recognizes that there is a substantial federal interest in promoting fair competition in the provision of wireless services and in ensuring the consumer confidence necessary to ensure continued growth in the use of wireless services. These goals can be attained by establishing a set of privacy rules that apply to wireless location information, regardless of technology, and to all entities and services that generate or receive access to such information. Further, the Act recognizes that it is in the public interest for the FCC to establish comprehensive rules to protect the privacy of customers of location-based services and applications and thereby enable customers to realize more fully the benefits of location services and applications.

3.1.2 European and Canadian Frameworks

In other jurisdictions, lawmakers have not consistently addressed locational privacy. In the European Union, some states have extended the general protection for location information under the EU *Data Protection Directive*.[8] Under this Directive, individuals must be informed and provided with a chance to object before their personal information – which includes location information – can be transferred to a third party. The EU Parliament also enacted similar provisions to 47 U.S.C. 222, providing that public telephone networks must comply with the Directive's constraints on the processing of personal data when making emergency location information about mobile subscribers to appropriate authorities. Further, the EU's *Directive for the Protection of Data and Privacy in the E-Communications Sector* establishes an opt-in requirement for the use of personal data in electronic communications consistent with the general directive.[9]

In Canada, regulators – such as the Canadian Radio and Telecommunications Commission (CRTC) – have yet to address the issue of locational privacy with legislation. Rather, the issue has been addressed on a case-by-case basis, some through the Canadian Wireless Telecommunications Association.[10] For example, the Office of the Privacy Commissioner of Canada (OPC) recently addressed locational privacy issues in a case involving the complaints of employees of a telecommunications company that installed Global Positioning System (GPS) devices in work vehicles. Specifically, the OPC assessed whether the information being collected via GPS is personal information as defined in section 2 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The OPC held that since the information could be linked to specific employees driving the vehicles, they are *identifiable* even if they are not identified at all times to all users of the system.[11] This issue of whether location is considered "identifiable" has and will become a common issue for users who wish to exercise their privacy rights with new geospatial applications.

3.1.3 Recommendations for Future Legal Framework

Although the US, EU, and Canada all have some legislation or approach to dealing with location-based applications, none of these jurisdictions have enacted legislation that specifically addresses the privacy issues associated with this emerging technology. Given the early stages of development of location-based applications, Anzen has prepared the following recommendations for the Federal Trade Commission to consider in determining next steps to address these applications.

---

[8] Council Directive 95/46/EC, 1995 O.J. (L 281).

[9] http://epic.org/privacy/location/jwhitelocationprivacy.pdf

[10] *What Happens When You Make A 911 Call? Privacy & The Regulation of Cellular Technology in the US & Canada*. http://web.uvic.ca/polisci/bennett/pdf/911Call.pdf

[11] PIPEDA Case Summary #2006-351 – Use of personal information collected by GPS considered (November 9, 2006).

First, Anzen recommends that the FTC explore the need for regulation of location-based applications. This includes asking whether specific legislation is required to properly address the privacy issues associated with location-based applications. Further, we recommend that the FTC ask whether self-regulation is a suitable alternative to legislation. In doing so, the FTC should consider whether the problems associated with self-regulation (e.g. lack of enforcement) would detract from this approach.

Second, Anzen recommends that the FTC engage the companies developing location-based applications in the process for exploring regulatory needs so that they can understand the privacy issues in the early stages and feel a greater involvement in determining, and therefore a greater likelihood in following, best practices.

Finally, it is our view that the FTC should consider the following issues in determining the best approach for regulation:

- The method for authorization (e.g. express, opt-in) for users of location-based applications;
- The type of notice and content of notice that providers of location-based applications will be required to give users about proposed uses of their personal location data (also discussed in section 3.2 below);
- What restrictions will be placed on third parties with respect to disclosing location data without the user's prior authorization; and
- The methods that providers should use for the deletion and deactivation of user accounts.

3.2 Informed Consent

This section addresses the extent to which location-based applications obtain users' consent to collect, use, and disclose their location and other related information. In doing so, Anzen discusses the importance of consent in personal information protection legislation and provides examples of consent frameworks in US and Canadian legislation. Then, Anzen explains how current location-based applications obtain consent from users. This section concludes with recommendations for how companies developing location-based applications may better obtain informed consent from users.

3.2.1 Collection, Use, and Disclosure of Personal Information via Location-Based Applications

Many location-based applications, such as those discussed in section 2 above, are "opt-in" applications. This means that an individual takes some positive action in choosing to sign up to use these applications and provides some sort of consent for the collection, use, and disclosure of location data. This contrasts to "opt-out" applications, where the user must actively decline location data from being shared with others and must also be able to specify when they no longer wish their location data will be stored. However, the extent to which the consent provided is informed or knowledgeable is not always clear and is not consistent among applications. For example, users consent to use Google Latitude by signing up by downloading the application from their mobile devices. The Google Mobile Privacy Policy[12] addresses Google's collection, use, disclosure, and retention of location-based information via Latitude and other mobile applications. However, it is unclear whether Google's Mobile Privacy Policy supersedes the privacy information provided in its Latitude tutorials and documentation. This means that the user may not

[12] Google's Mobile Privacy Policy is available at: http://m.google.com/static/en/privacy.html.

completely understand what information Google collects from him or her and how this information is used.

3.2.2 The Importance of Consent

Consent is the general focus of personal information protection legislation in that it allows users to exercise control over their personal information. For example, in the US, the *Privacy Act of 1974* states that no federal agency may disclose information without the consent of the person.[13] Further, the *Health Insurance Portability and Accountability Act of 1996* is also a consent-based statute, but enables covered entities to use personal health information without an individual's consent for the purposes of providing treatment to the individual, for payment activities, and for operating their businesses.

The bedrock of Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) is individual consent, which can be express or implied, depending on the circumstances.[14] Even when consent is obtained, businesses must limit the collection, use, and disclosure of personal information to purposes that a reasonable person would consider appropriate under the circumstances. Under PIPEDA, the "reasonable person" test is central to privacy protection and is applied contextually in each case to strike the appropriate balance between individual privacy concerns and business interests.[15] The Office of the Privacy Commissioner of Canada (OPC) also focuses on whether consent is *meaningful* and will generally consider consent to be meaningful if the individual in question is informed in a clear and understandable manner of the purposes for collecting, using, and disclosing personal information, prior to any such collection, use or disclosure of personal information.

PIPEDA and other Canadian privacy legislation, such as Ontario's *Personal Health Information Protection Act*, distinguish between "informed" and "knowledgeable" consent. Informed consent requires an organization to identify the reasonably foreseeable consequences of collections, uses, and disclosures of personal information. Knowledgeable consent, on the other hand, may be obtained when the user knows the purposes of the collection, use, or disclosure, and that the user may give or withhold consent.[16] According to the OPC's Guide for Businesses, businesses should obtain consent by:

- Informing the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data; and
- Obtaining the individual's consent before or at the time of collection, as well as when a new use is identified.

Businesses may fulfill these responsibilities in several ways, including by communicating in a manner that is clear and can be reasonably understood, recording the consent received (e.g. note to file, copy of e-mail, copy of check-off box), and explaining to individuals the implications of withdrawing their consent.[17]

---

[13] Electronic Privacy Information Center: http://epic.org/privacy/medical/.

[14] OPC Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act Fact Sheet. http://www.priv.gc.ca/fs-fi/02_05_d_24_e.cfm.

[15] OPC Fact Sheet: Complying with the Personal Information Protection and Electronic Documents Act. http://www.priv.gc.ca/fs-fi/02_05_d_16_e.cfm.

[16] Halyna Perun, Michael Orr, & Fannie Dimitriadis. *Guide to the Ontario Personal Health Information Protection Act*. Toronto: Irwin Law, 2005. Pp. 198-199.

[17] Privacy Commissioner of Canada: http://www.priv.gc.ca/information/guide_e.cfm#008.

3.2.3 Current Methods of Obtaining Consent

Companies offering location-based applications currently use varying methods to inform users of the collection, use, and disclosure of their information and their options for controlling this information. Some of these methods are as follows:

- Google includes its information management practices in relation to Latitude in Latitude tutorials and "Help" frequently asked questions. In addition, the Google Mobile Privacy Policy[18] addresses Google's collection, use, disclosure, and retention of location-based information via Latitude and other mobile applications.
- Foursquare informs users through the Terms of Use and Privacy Policy, which is found on its website.[19]
- Brightkite has a privacy policy[20] that outlines, among other things, the distinction between personal and non-identifying information, the uses of "log data", its disclosure of aggregate and non-identifying information, and how users may change or delete information.

From a privacy perspective, these companies have generally taken a positive approach by asking users to opt in to their applications. However, there is a disparity in how these new companies are addressing the collection, use, and disclosure of personal information in their privacy policies. While Brightkite makes an effort to address this, there are still some gaps in its policy. For example, Brightkite addresses the deletion and deactivation of user profiles as follows: "If you would like us to delete your record in our system, please contact us and we will attempt to accommodate your request if we do not have any legal obligation to retain the record." While this is helpful, it is not an explicit promise that user data will, in fact, be deleted.

Further, although some policies discuss identifiable and non-identifiable information, these policies do not include how this information may become identifiable when combined with other information to make inferences. For example, if a location-based application tracks that a user attends at a kidney dialysis clinic two or three times a week for several hours, then it may reasonably be inferred that this user is a dialysis patient.

3.2.4 Recommendations for Obtaining Consent in Location-Based Applications

Businesses want to ensure that users understand what they are consenting to when they sign up for their location-based applications in order to build consumer trust and to prevent consumer complaints in the future. For example, in its recent decision surrounding the privacy practices of Facebook, the OPC discussed the methods of informing users about the purposes of the collection, use and disclosure of their personal information in the context of social media applications. The OPC noted that, like the companies responsible for location-based applications, Facebook informs users of its purposes via the privacy policy, terms of service, and other documents. In their decision, the OPC made several recommendations to Facebook that seek to ensure that users have the information they need to make meaningful decisions about how open they wish to be in sharing their personal information. Although the OPC recommends "real-time" notification, they appreciate that Facebook wants to obtain consent while providing users with a seamless experience.[21]

In order to ensure that users of location-based applications understand how their information is collected, used, and disclosed, Anzen recommends that the FTC consider how consent fits into

---

[18] Google's Mobile Privacy Policy is available at: http://m.google.com/static/en/privacy.html.

[19] Foursquare Privacy Policy: http://foursquare.com/terms#privacy.

[20] Brightkite Privacy Policy: http://brightkite.com/pages/bk_privacy_policy.html.

[21] PIPEDA Case Summary 2009-008: http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm.

regulation. As discussed in section 3.1 above, we understand that the FTC is still in the early stages of addressing this emerging technology and needs to consider options for education, regulation, and/or self-regulation. It is Anzen's view that the issue of consent would be best addressed by companies in privacy policies and notices. To this end, Anzen recommends that the FTC consider the following in developing guidelines for privacy policies for location-based applications:

- **Clear notices:** Companies should develop clear privacy policies or amend existing privacy policies to address identifiable information, ownership of information, and potential and future uses of information. These policies should outline *all* collections, uses, and disclosures of personal information and may be specific to applications, rather than suites of applications.
- **Opt-in mechanisms:** The location-based applications discussed in these comments are generally opt-in applications. These companies should be commended for implementing privacy and consent procedures early on in the deployment of these location-based applications. Based on this practice, Anzen recommends that the FTC establish opt-in as the standard for location-based applications and establish a practice of having users review an application's privacy policy prior to signing up for and consenting to use the application.
- **Deletion and Deactivation:** One of the privacy concerns behind location-based applications is that the information collected for the primary purpose of the application (e.g. serving information to users based on users locations) will be used for other purposes through, for example, data linking and aggregation. To this end, it is important to provide users with the option of deleting and/or deactivating their account, such that their identifiable information no longer exists in any application and that this information can no longer be accessed by anyone.
- **Contact person:** It is a common privacy best practice to appoint a contact person to handle privacy inquiries and complaints. For example, Brightkite provides a telephone number and email address in its Privacy Policy for this purpose. As such, Anzen recommends that the FTC encourage companies offering location-based applications to appoint a contact person and make this individual's information publicly and easily available.

3.3 Aggregating Location-Based Information

In this section, Anzen discusses how location-based information is typically aggregated and used for secondary purposes and the privacy issues that arise from this practice. For the purposes of our comments, Anzen defines the aggregation of location-based information as the combining of geospatial information, such as geographic coordinates or maps, with any other type of potentially identifiable personal or statistical information, such as name and address, demographics, crime statistics, or user-generated content.[22] This section also focuses on geo-browsers, such as Google Streetview and My Maps (discussed in section 2 above), because they provide one means for aggregating location-based information. Finally, this section concludes with Anzen's recommendations for the FTC's Privacy Roundtable discussion on the topic of aggregating location-based information.

3.3.1 Function Creep

The convergence of location-based applications with government and publicly-available information has presented new opportunities and benefits ranging from health care initiatives that can save lives, improve patient safety, and minimize infectious disease outbreaks to market analysis that enables companies to identify market opportunities and optimize capital investments and revenue. However, this convergence is also giving rise to mass databases, complex data

[22] User generated content refers to any information that is published on the internet by an end-user, including blogging, online posts, wikis, mobile phone photography, and podcasting, among other things.

uses and disclosures, and, consequently, privacy issues. One major issue that reveals privacy concerns is "function creep", a term that refers to the progressive propensity to use information systems or processes for other purposes that were not part of the original design strategy.[23] In the context of location-based applications, function creep includes the unintended aggregation of location-based information for secondary uses. These might include, for example, disclosures of location-based information by custodians to law enforcement agencies or third party marketers, who then aggregate this information for criminal investigations or market research, respectively.[24]

3.3.2 Sources for Aggregating Location-Based Information

The availability of geographic and statistical information, whether over the internet or otherwise, has increased exponentially over the past twenty years. Digital cameras, mobile phones, satellite navigation systems, and other common devices have enabled mass collection and aggregation of location-based information with other personal information, such as user generated content. At the same time, online mapping interfaces, which enable users to produce and share aggregated location-based information, have become progressively more user-friendly. This is aided by the fact that geo-browsers provide an easy-to-use platform for less tech-savvy users to overlay information on mapping interfaces. Now, companies are encouraging greater user participation in product development by willingly sharing location-based and other information to enable users to create new re-composed content. Users are also generally more willing to provide personal information for mapping purposes, particularly to obtain valuable information or services. For instance, mobile phones containing Global Positioning Systems (GPS) can automatically record personal location coordinates when a picture is taken and cyclists can map out and share their routes over the internet.[25]

In addition to these burgeoning sources of location-based information, companies and users can also access this information from more conventional sources, such as from the government either via the web or by visiting local town halls.[26] This information might include, for instance, population, economic, industry, and geographic studies from the US Census Bureau or land registry information containing the names of previous and current property owners, as well as information about their liens, mortgages, and debentures. For example, users could access this information and subsequently link it with base maps of various cities or states in the US.[27]

Private sector companies are also collecting location-based information through location-based applications, RFIDs, and cell phone tracking. They also collect field information through the use of GPS devices attached to particular features (e.g. pump station, vehicles, or persons), which then record their corresponding coordinates over space and time.[28] Some companies then sell this location-based information to third parties for commercial purposes, such as marketing.[29]

---

[23] Oxford Learner's Pocket Dictionary of Business English. http://www.oup.com/elt/catalogue/teachersites/oald7/wotm/wotm_archive/function_creep?cc=global.

[24] Office of the Privacy Commissioner of Canada. "Geospatial Workshop Report." 10 June 2009.

[25] Mark Burdon. "Privacy Invasive Geo-mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws." University of Illinois Journal of Law Technology and Policy 2010(1) (In Press). http://www.jltp.uiuc.edu/works/Burdon.htm.

[26] ESRI. "GIS Best Practices: Essays on Geography and GIS." September 2008. http://www.esri.com/library/bestpractices/essays-on-geography-gis.pdf.

[27] ESRI. "GIS Best Practices: Essays on Geography and GIS." September 2008. http://www.esri.com/library/bestpractices/essays-on-geography-gis.pdf.

[28] ESRI. "GIS Best Practices: Essays on Geography and GIS." September 2008. http://www.esri.com/library/bestpractices/essays-on-geography-gis.pdf.

[29] Office of the Privacy Commissioner of Canada. "Geospatial Workshop Report." 10 June 2009.

3.3.3 Methods for Aggregating Location-Based Information

Once companies or the public collect the information from any of the above sources, they may then combine one or more data streams onto a geographical interface. Companies generally utilize what is called a Geographic Information System (GIS) to integrate geographic data onto a project map and, subsequently, process, capture, manage, analyze, and display it.[30] Typically, GIS packages include map file databases, which serve as additional sources of geographic information for companies.[31]

Some companies are devoted to providing clients with these data aggregation services. For instance, DMTI Spatial Locations Intelligence Solutions is a company that combines location-based data with other databases to help its clients identify market and customer opportunities and optimize capital investments and assets, among other things.[32] Marketers, in particular, are increasingly employing the use of location-based applications, particularly GIS, to reveal relationships, patterns, and trends in the form of maps, charts, and reports.[33] For example, Equifax and National Decision Systems released Infomark-GIS in 1993. Infomark-GIS combines the functionality of Infomark (a desktop marketing information system from National Decision Systems) with ArcInfo (GIS software). Specifically, it provides a "GIS solution with comprehensive national databases, industry-specific applications, sophisticated mapping tools, plus the ability to integrate your own internal data."[34] Infomark-GIS offers location-based information through a variety of sources, including Bing Maps. It may also use the US National Decision Systems' EQUIS database, as it includes a wealth of financial, demographic, credit card activity, buying activity, and credit relationship information on approximately 100 million Americans.[35] The use of GIS enables marketers to maintain their competitive edge by better understanding consumer interests and, subsequently, marketing products and services tailored to those consumer interests.[36]

3.3.4 Privacy Issues

The aggregation of location-based information for secondary purposes poses the following privacy concerns to individuals:

- **Revealing an Individual's Physical Location:** Both companies and public users have developed websites that track the movement of specific individuals by aggregating location-based information onto geo-browsers. This can create detailed databases linked to the name of an individual. Further, it can create longitudinal personally-identifying records of an individual's movement in space and time.[37] This form of data aggregation does not necessarily involve the attachment of a GPS device to a particular individual, but may only require concerted efforts by users to continually input location-based data about that

---

[30] ESRI. "What is GIS?" http://www.gis.com/whatisgis/index.html.

[31] ESRI. "GIS Best Practices: Essays on Geography and GIS." September 2008. http://www.esri.com/library/bestpractices/essays-on-geography-gis.pdf.

[32] DMTI Spatial Solutions. "DMTI Spatial Solutions: A Unique Approach for Proven ROI." http://www.dmtispatial.com/en/Solutions.aspx.

[33] ESRI. "What is GIS?" http://www.gis.com/whatisgis/index.html.

[34] Equifax National Decision Systems. InfoMark-GIS: Tomorrow's Technology for Today's Business Success." Atlanta, GA (1993): Equifax, Inc. http://legacy.library.ucsf.edu/tid/yfn50b00/pdf.

[35] George Cho. "Location and Privacy Issues." Coordinates. January 2008. http://www.mycoordinates.org/location-and-privacy-issues.php.

[36] George Cho. "Location and Privacy Issues." Coordinates. January 2008. http://www.mycoordinates.org/location-and-privacy-issues.php.

[37] Office of the Privacy Commissioner of Canada. "Geospatial Workshop Report." 10 June 2009.

individual. This is a particularly popular practice for tracking celebrity sightings and local eccentrics. For instance, a media website called Gawker tracks celebrities in New York or Los Angeles by allowing users to input information about the location, time, data, and other sighting details. This information is updated every fifteen minutes and then interfaced onto Google Maps.[38] This raises the issue of using location-based applications to collect and compile a large amount of publicly-available information (e.g. seeing a celebrity at a restaurant), which can invade an individual's privacy.

There are also risks to the personal privacy of consumers when geospatial information is aggregated with data derived from online stores and websites. This can occur even when information from the websites themselves may not be personally identifying or privacy-invasive. For example, one author linked "wish list" information from Amazon books with personally identifying information using Yahoo People Search and, then, associating that information with a specific satellite image of that user's residence on Google Maps.[39] Thus, aggregating information using various sources can establish a consumer's identity, location, and personal buying preferences.

In addition, marketing companies aggregate location-based data with demographic information using GIS in order to determine geographic regions that are more likely to respond to a particular advertisement. Many individuals argue that the use of this information for directed or tailored marketing not only is unauthorized but is also a form of discrimination and an invasion of individual, and the community's collective, privacy.[40]

- **Perpetuating Discriminatory and Erroneous Information:** Users may anonymously submit sensitive and potentially discriminatory information on websites in a way that enables other users (e.g. media and corporate outlets) to combine it with location information and publicly share the results over the internet. In some cases, aggregating data in a particular manner has led to damaging consequences. For example, information about British National Party (BNP) membership in the UK was leaked through Wikileaks and subsequently aggregated by the Times with postal code information on Google Maps. As a result, members experienced termination of employment, death threats, and property damage. Further, areas where BNP members lived were illustrated on the maps as a single point – thereby attributing the area to a single resident who may or may not have been a member of the BNP. This led to targeting of residents who were not connected with the BNP.
- **Revealing Information about At-Risk Populations:** Police departments, news reports, and user-generated content have recently been used to develop websites, such as SpotCrime, that overlay crime details, statistics, and event coordinates onto geo-browsers, such as Google Streetview. The purposes of these websites are to provide the public with location-based crime statistics and up-to-date information. Although developers of these programs recognize the need to redact certain sensitive information, there remains a real risk of identifying or re-identifying victims. For instance, one researcher was able to identify the residence of a rape

[38] Mark Burdon. "Privacy Invasive Geo-mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws." University of Illinois Journal of Law Technology and Policy 2010(1) (In Press). http://www.jltp.uiuc.edu/works/Burdon.htm.

[39] Mark Burdon. "Privacy Invasive Geo-mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws." University of Illinois Journal of Law Technology and Policy 2010(1) (In Press). http://www.jltp.uiuc.edu/works/Burdon.htm.

[40] Alastair R. Beresford. "Chapter 13: Privacy Issues in Geographic Information Technologies." Privacy Issues in Geographic Information Technologies. Ed. Sanjay Rana and Jayant Sharma. Springer: Berlin, 2006.

victim via Google Streetview even though the victim's address information had been partially redacted.[41]

- **Persistence of Sensitive Information on the Internet:** As indicated above, information that is superimposed onto geographic interfaces can remain on the internet indefinitely as users continue to integrate it with other information. This is a particularly serious issue when it involves sensitive location-based information, such as information relating to vulnerable groups such as children and abused women.[42,43] For example, women's shelters have asked for companies to remove their location-based information to protect the safety and privacy of visitors and clients. However, because this information is already harvested by other sites, it is nearly impossible to remove it from all the locations where it has subsequently been posted. Similarly, when teachers used My Maps to customize directions for visits to various students' homes, they were unable to subsequently delete the home addresses of their students because the information was made available in the public domain via My Maps. At the time, the teachers were unaware that information on My Maps is made available to all users, when default settings are activated, and that it is difficult for Google to delete this information because it is stored on more than one server. This has also occurred with renal disease patients receiving dialysis in Japan. [44] This trend suggests that companies might not be providing clear privacy notices and user control over their information. It also indicates a lack of regulation over internet data matching, within North America and abroad.[45,46]

3.3.5 Recommendations for Data Aggregation

Location-based data aggregation can provide companies and users with valuable tools and services. As such, it is Anzen's view that it is important to advance privacy protective measures in this area without stifling innovation. In order to do this, Anzen recommends that the FTC's discussion with key stakeholders including, among others, major geo-browsers, privacy advocates, other collaborating oversight agencies, privacy organizations, advertising associations, and the community of users engaging in location-based data aggregation and include a discussion of the following issues:

- **Public Education:** There is currently little public education about the privacy issues associated with location-based data aggregation. It is Anzen's view that stakeholders consider how industry and oversight agencies might effectively communicate and increase the public's knowledge and awareness of the major issues (e.g. risks of (re)identification and inability to delete information). This will better inform the public of the consequences of user-posted information and the aggregation and use of location-based information for secondary purposes.

  The internet is providing users with a vast array of information that can be aggregated more easily and in more ways than before, thereby making it difficult to control data aggregation in

---

[41] Mark Burdon. "Privacy Invasive Geo-mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws." University of Illinois Journal of Law Technology and Policy 2010(1) (In Press). http://www.jltp.uiuc.edu/works/Burdon.htm.

[42] Office of the Privacy Commissioner of Canada. "Geospatial Workshop Report." 10 June 2009.

[43] Office of the Privacy Commissioner of Canada. "Geospatial Workshop Report." 10 June 2009.

[44] Mark Burdon. "Privacy Invasive Geo-mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws." University of Illinois Journal of Law Technology and Policy 2010(1) (In Press). http://www.jltp.uiuc.edu/works/Burdon.htm.

[45] George Cho. "Location and Privacy Issues." Coordinates. January 2008. http://www.mycoordinates.org/location-and-privacy-issues.php.

[46] "Misuse of Location-Based Services and Human Trafficking: Prevention and Solutions." Davey Jones' Locker Site. Oregon State University. December 2005. http://dawn-drupal.science.oregonstate.edu/solutions.

a way that protects personal privacy. To this end, Anzen also recommends that stakeholders educate users about proper conduct and ethical practices associated with aggregating location-based information.

- **Transparency and Individual Control:** Similarly, Anzen recommends that companies offering geo-browsers take steps to clarify how user-posted, location, and personal information will be used and disclosed, as well the ability for users to delete or remove this information.
- **Accountability**: Anzen recommends that the education, regulatory, and/or self-regulatory framework discussed in section 3.1 above address the above-mentioned uses of location-based information, with a focus on sensitive and at-risk populations.
- **Innovative Solutions:** Engaging with conceptual thinkers and technology developers working in this area can help create equally as innovative advancements that help resolve or mitigate the privacy risks both unique to location-based data aggregation and otherwise. Some groups are currently working towards developing privacy enhancing solutions and techniques that can be embedded into location-based applications and services. For instance, Janice Warner and Soon Ae Chun promote the concept of interacting privacy policies, which ensures privacy protection by representing the interests of different parties involved in the location-based data aggregation process.[47] More specifically, this solution involves a network of personal privacy policies that enables users to submit their privacy preferences so they can later be interpreted and enforced by a privacy enforcement engine.[48] In addition, Jonathan Zittrain encourages the development of privacy tags, which are tagged meta-data that would signal whether data being collected, used, or disclosed is permitted, whether individuals prefer to remain linked with the information uploaded on the internet, and whether they prefer to be consulted about any abnormal future collections, uses, or disclosures.[49,50]

---

[47] Janice Warner & Soon Ae Chun. "A Citizen Privacy Protection Model for E-Government Mashup Services." *Information Polity.* 2008.

[48] Mark Burdon. "Privacy Invasive Geo-mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws." University of Illinois Journal of Law Technology and Policy 2010(1) (In Press). http://www.jltp.uiuc.edu/works/Burdon.htm.

[49] Jonathan Zittrain. The Future of the Internet – and How to Stop It. (Virginia: R.R. Donnelley, 2008).

[50] Mark Burdon. "Privacy Invasive Geo-mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws." University of Illinois Journal of Law Technology and Policy 2010(1) (In Press). http://www.jltp.uiuc.edu/works/Burdon.htm.

4 Anzen Team

Miyo Yamashita, PhD: Miyo Yamashita is the founding partner of Anzen and has a Ph.D. in Communications from McGill University, where she specialized in the impact of data protection laws on privacy practices. Miyo has been working in the information privacy field since 1990, during which time she has designed and implemented corporate privacy programs, conducted dozens of privacy impact assessments, legislative reviews, gap assessments, and developed strategic privacy plans for governments, health care delivery organizations, the private sector, and charities.

In September 2001, Miyo was hired as the first Corporate Privacy Officer (CPO) at University Health Network, one of the Canada's largest teaching hospitals. In her role as CPO, Miyo managed the departmental operating budget, conducted privacy impact assessments on the hospital's various clinical and business information systems, investigated privacy complaints, developed an employee privacy training program with web-based tutorials, served on the hospital's Research Ethics Board as a privacy advisor, implemented a patient communications and education strategy on privacy, developed data protection guidelines for the hospital's electronic patient record system, and worked jointly with the Information and Privacy Commissioner/Ontario on an independent assessment of privacy practices at the hospital.

Megan Brister, CISSP, PMP: A partner with Anzen, Megan has built a career in the data protection field working with both private and public organizations to develop cost-effective, practical privacy and information security programs. Megan has conducted dozens of privacy impact assessments for government, health care delivery organizations, and information technology firms. In addition, Megan has developed and implemented privacy programs for several clients as well as acted in the role of Privacy Officer for each organization.

Prior to joining Anzen, Megan worked as the Director of Data Protection for MDS Inc., a global health and life sciences company, where she developed a global data protection program to oversee compliance of information systems and information network providers with Canadian, US, and European data protection laws. Megan guided privacy components of large infrastructure projects and advised on issues such as outsourcing, international data transfer, security, and compliance with the Personal Information Protection and Electronic Documents Act, the US Health Insurance Portability and Accountability Act, provincial health information privacy statutes, and self-certification schemes such as Safe Harbor.

Megan also has over ten years of project management experience and is a Certified Information Systems Security Professional (CISSP) and Project Management Professional (PMP).

Don MacPherson, BSc: Don is a partner at Anzen and a graduate in Health Information Science from the University of Victoria. Don specializes in providing clients with strategic privacy, information governance, data protection, and risk management advice. As a nationally recognized information privacy advisor, Don has co-authored several privacy reference documents for the health care sector, including Canada Health Infoway's Interoperable Electronic Health Record Privacy and Security Requirements, Privacy and Security Conceptual Architecture, White Paper on Information Governance, and a Conceptual Privacy Impact Assessment on a Pan-Canadian Interoperable Electronic Health Record. Don has completed numerous privacy impact assessments and developed several privacy programs for regional, provincial, and national e-Health initiatives.

Don began his privacy career as a Privacy Specialist at University Health Network, where he worked with the hospital's Corporate Privacy Officer to conduct privacy impact assessments on the hospital's various clinical and business information systems, investigated staff and patient privacy complaints, implemented a patient communications and education strategy on privacy,

and worked jointly with the Information and Privacy Commissioner/Ontario on an independent assessment of privacy practices at the hospital.

Jeffrey Cutler, LLB: Jeffrey is a lawyer with Anzen who specializes in information privacy. Jeffrey assists clients with compliance reviews, privacy policy development and implementation, privacy communications plans, and training material. At Anzen, Jeffrey has conducted statutory privacy reviews and assessments for clients who operate across Canada and internationally.

Prior to joining Anzen, Jeffrey was an Investigator with the College of Nurses of Ontario, where he advised health care professionals, patients, and regulators on their roles, responsibilities, and rights concerning the protection of personal health information. In Newfoundland and Labrador, Jeffrey held the role of legal counsel with the Newfoundland Human Rights Commission and policy analyst with the Government of Newfoundland and Labrador. In the latter role, Jeffrey assisted the Government of Newfoundland and Labrador in developing a strategy to address the *Personal Information Protection and Electronic Documents Act* and in drafting electronic commerce legislation.

Jeffrey is a graduate of Memorial University of Newfoundland and holds a law degree from Dalhousie University, where he also received a Health Law Specialization Certificate. He is a member of both the Law Society of Upper Canada and the Law Society of Newfoundland and Labrador.

Beth Dewitt, MA: Beth is a privacy specialist who focuses on privacy program development and implementation, privacy training, and privacy breach management. Beth has trained several Privacy Officers to manage their organizations' privacy plans and programs, as well as acted as an interim Privacy Officer until clients were able to fill these roles.

Beth also specializes in advising clients on information governance, consent, and privacy statutory issues involved in the implementation and deployment of large provincial and national information technology solutions.

Beth holds a Master of Arts in Social Anthropology and a Graduate Diploma in Health Services and Policy Research from York University.

Michelle Gordon, LLB: Michelle is a privacy lawyer with Anzen who specializes in information and privacy governance. Prior to joining Anzen, Michelle practiced civil and employment litigation and also worked at a large international law firm, where she assisted in advising private sector clients on their responsibilities under new federal and provincial privacy legislation including the *Personal Information Protection and Electronic Documents Act* and the *Freedom of Information and Protection of Privacy Act*. Michelle also interned at the Electronic Privacy Information Center in Washington, D.C., where she contributed to projects on the US *Freedom of Information Act* and the *Health Insurance Portability and Accountability Act of 1996* and researched and wrote on emerging civil liberties issues relating to privacy and anonymity.

Since joining Anzen, Michelle has conducted privacy impact assessments for national, North American, and international organizations in order to help them understand the privacy governance framework under which they may operate, their legislative requirements, and the practical privacy solutions they may employ to protect personal information.

Michelle holds a B.A. from the University of Toronto and an LL.B. from the University of Ottawa. During law school, Michelle was a researcher in privacy and technology law for Professor Michael Geist and completed a major research paper on the privacy implications of radio-frequency identification technology under the supervision of Professor Ian Kerr. Michelle is presently working towards a Master of Laws degree, with a focus on privacy and health law, from the University of Toronto.

Sylvia Kingsmill, LLB: A privacy lawyer at Anzen, Sylvia specializes in providing strategic risk management and privacy advice. Sylvia has extensive knowledge of privacy legislation and its application to technology initiatives, specifically in creating data protection regimes and accountability frameworks for provincial and national research registries. She also assists clients with organization-wide privacy policy development and implementation, privacy breach management, data sharing agreements, as well as privacy communications plans and training programs.

Prior to joining Anzen, Sylvia was a Communications Specialist at the Information and Privacy Commissioner/Ontario (IPC), where she also served as the Commissioner's Executive Assistant. At the IPC, Sylvia was responsible for the development and implementation of a provincial educational strategy for the *Personal* Health Information Protection Act, 2004 (PHIPA). She authored extensive PHIPA internal and external communications tools and provided guidance to health care practitioners and organizations on the application of PHIPA.

Sylvia is a graduate of York University (B.A., Hon.) and has a law degree from the University of Ottawa, where she specialized in Corporate Law. She was called to the Ontario Bar in 2003 and is a member of the privacy law section of the Ontario Bar Association.

Jordan Prokopy, MA: A privacy specialist at Anzen, Jordan has conducted privacy impact assessments, privacy gap assessments, and privacy audits for private sector and government organizations. Jordan's focus is on the privacy issues surrounding the management of personal information for customer service and marketing. Jordan also specializes in online behavioral advertising, particularly the privacy best practices and regulatory requirements for advertising networks, advertising exchanges, and publishers.

Jordan also brings in-depth bioethics and research expertise to the field of health privacy. A trained bioethicist, Jordan, advises health care and health research clients on privacy program development, consent management, information governance, and data sharing agreements.

Prior to joining Anzen, Jordan served as the ethicist on the Montreal General Hospital's Research Ethics Board where she advised on ethical standards and practices for research, including privacy, security, and confidentiality practices. Jordan also conducted research in the areas of living unrelated kidney donation and the ethical issues and practical challenges of "whole person care".

Jordan has a Master's of Arts in Biomedical Ethics and a Bachelor of Science in Biology and Mathematics from McGill University.

Naomi Zittell, LLB: Naomi is a privacy lawyer with a specialized understanding of health information privacy issues and national and international privacy laws. Before joining Anzen, Naomi practiced law at a Toronto-based litigation firm, where she represented a diverse cross-section of individuals and corporations.

At Anzen, Naomi has assisted Ontario's Colorectal Cancer Screening Program to gain the approval of the Information and Privacy Commissioner/Ontario to operate as a "prescribed registry" under Ontario's health privacy legislation. In addition, she developed the privacy program and trained its Privacy Specialist and staff.

Naomi has also conducted privacy impact assessments for multiple municipal, national, and international organizations. Naomi is a frequent speaker at privacy conferences and has led employee privacy training sessions for several clients.

Naomi is a graduate of McGill University, where she completed her degree in North American Studies, and of the University of Ottawa's Faculty of Law, where she studied both privacy law and health law. Naomi is a member of the Ontario Bar Association and has training in alternative dispute resolution.