PRIVACY PROTECTION IN GEOLOCATION MONITORING APPLICATIONS

By

Kush Patel (143672)

kpatel4@student.concordia.ab.ca

Krishna Vyas (144499)

kvyas@student.concordia.ab.ca

Dhruv Vyas (144303)

dvyas@student.concordia.ab.ca

Monika Patel (144068)

mpatel6@student.concordia.ab.ca

Research Project

Submitted to the Faculty of Graduate Studies

Concordia University of Edmonton

In Partial fulfillment of the Requirements for the final

Research Project (ISSM581(R))

Department of Information Systems Security Management

Concordia University of Edmonton, Edmonton T5B 4E4, Alberta, Canada

Advisor: Dr Sergey Butakov

sergey.butakov@concordia.ab.ca

June 2021

Privacy Protection in Geolocation Monitoring Applications

Kush Patel

Krishna Vyas

Monika Patel

Dhruv Vyas

Approved:

Sergey Butakov [Original Approval on File]

Sergey Butakov — Date: June 23, 2021
Primary Supervisor

Patrick Kamau [Original Approval on File]

Patrick Kamau, PhD, MCIC, PChem. — Date: June 23, 2021
Dean, Faculty of Graduate Studies

Table of Content

List of Figures

List of Tables

Privacy Protection in Geolocation Monitoring Applications

Kush Patel
Concordia University of Edmonton
Edmonton, Canada
kpatel4@student.concordia.ab.ca

Monika Patel
Concordia university of Edmonton
Edmonton, Canada
mpatel6@student.concordia.ab.ca

Adviser: Dr Sergey Butakov
Concordia University of Edmonton
Edmonton, Canada
Sergey.butakov@concordia.ab.ca

Dhruv Vyas
Concordia University of Edmonton
Edmonton, Canada
dvyas@student.concordia.ab.ca

Krishna Vyas
Concordia University of Edmonton
Edmonton, Canada
kvyas@student.concordia.ab.ca

ABSTRACT

The use of geolocation tracking demands to have an understandable and robust privacy policy implemented along with these services. Many available policies may lack important statements to achieve this robustness, and some are too cumbersome for the end users to understand. A privacy policy template has been proposed in this research which is intelligible to the privacy policy developers and end-users. It includes all necessary information which a policy should have. Based on this template, two sample privacy policies also have been proposed. The aim of this project is to help developers make policies that will protect the organization from potential liabilities and help users understand how their data is being collected, stored, and processed in simpler words.

Keywords

Geolocation, Privacy Policy, Policy Template, Geolocation Tracking, Privacy laws, Location Based Services

1. INTRODUCTION

Due to the extreme extensive use of GPS (Global Positioning System), Wi-Fi (Wireless-Fidelity), wireless cellular networks, and IP location identification methods, a broad variety of generic technological apps are now feasible. Customizing information and services to consumers in specific locations, performing banking transactions with better certainty of wireless security from mobile devices, as well as utilizing the capability to synchronize devices including a variety of wireless platforms and location of the user via cloud storage [1].

Marketers, merchants, government bodies, law enforcement, attorneys, and unfortunately, criminals are all interested in using location technology to tailor a consumer experience. Despite their significant advantages, these services endanger the user, service providers, and those who rely on the data collected by the service providers. Many individuals and businesses have adopted this technology due to the potential benefits, resulting in increased data and personal privacy risks [1].

The privacy of such sensitive information of an individual is a major concern, and it needs to be protected so that the data does not get exposed. Geolocation refers to an individual's private space and location. It is used for identifying the place or the area where the individual resides and can be useful in tracking the whereabouts of an individual [2].

Other uses for geolocation data include localization of provided content, targeted advertising, access enforcement, e-discovery in favor of lawsuits and regulatory enforcement, geographic delivery restrictions, fraudulent detection and prevention, network traffic analysis, and real-time incident management via geolocation improvement of logs as well as other IT information. Expanding these techniques and related demand calls for increasing issue of the sensitivity of the data linked with them, which is frequently private and/or sensitive. To be able to utilize geolocation technologies properly, it is necessary to be extremely conscious of concerns connected to security and privacy [1].

These Location Based Service play a significant role for providing the geolocation-based information. There are many technologies that are used for LBS.

- Tracking via GPS – uses an array of satellites build for the purpose of finding this across the planet. A device with GPS receiver can ping multiple satellites to communicate. These satellites then compare the signal delays and can pinpoint location of the device.
- AGPS – Assisted GPS collects the location information from nearby cell towers and enhances the performance of standard GPS. When normal GPS signals are weak or absent, AGPS leverages proximity to cellphone towers to determine location.
- RFID – The RFID scanner has a static location. When the scanner is turned on, it may record the access and tag its position. This is used to determine where the device that is accessing the scanner is located.
- Wi-Fi access points/ IP address - Typically a device is connected to only one WI-FI network at a time, removing the potential of triangulation. This WI-FI network provides a physical IP address to the device from which current address is accessed.

Some of the organizations who use LBS, and geolocation tracking may take a fast-and-loose approach to privacy and fail to protect

user's privacy. There are many common issues these privacy policies have [3].

- Overuse of Legalese language. A language which only some technical professionals and lawyers understand.
- Not complying with Relevant Legislation. For example, organization needs to comply with 3 different legislations if they collect data from European residents, have a market for children and sell goods with California. Which many organizations fail to do.
- Missing Important Clauses. – Privacy policy should represent all the ways organization collects, stores, and uses the data. It should also include what happens with data if the organization's business is sold. Failure to include this information leaves the policy incomplete.
- Lack of information on how to contact the organization in case of privacy concerns.

To resolve these issues, a template has been proposed in this research. This template will help organizations to comply with relevant privacy laws, protect form liabilities, includes all important clauses, and is intelligible to an end user.

The following is how the rest of the paper is organized: Literature review outlines workings of IP geolocation tracking, and privacy related issues associated with them. It later discusses how a good privacy policy can help mitigate the issues. The Methodology section explains research process and address the issues involved in Geolocation tracking. It also defines the data collection methods and provides details on findings. The Template section of the research provides structure and detailed policies needed to resolve issues present in current policies regards to IP geolocation tracking. Application 1 & 2 sections outlines where IT geolocation tracking can be used and possibilities of users being unaware of their personal information usage. The conclusion part summarizes achievement of research aim and objectives.

2. LITERATURE REVIEW

Privacy related risks have been escalated exponentially in this era of digitalization. Maintaining the Confidentiality, Integrity and Availability of the Organization can be obtained by putting privacy rules into considerations. The privacy of the data is a paramount concern for any organization, and hence it must be protected so that the data does not get revealed [4].

Privacy of an individual's location refers as Geolocation privacy is utilized for identifying the place where the individual exists in. Geolocation makes use of the Global Positioning System (GPS) which is installed in most of the electronic devices to track locations. The GPS comprises of satellites that gets the specific location of an individual and to keep a track of their movements.

Depending on the location of an individual, it can be utilized to recognize in which country, continent, state, or city the person is in. At times persons are asked to agree to the terms and conditions related to provide their location. It is possible to find out where a person is using the applications that have the geolocation enabled [2].

Though the information is utilized for the purpose of marketing, there are many ways in which the data can be misused. To protect the data related to the privacy and to develop and refine representations of the location in the IP's as well as to assure that the Confidentiality, Integrity, Availability, and authorization conditions are satisfied, the concept of Geopriv - Geolocation Privacy.

To take care privacy regarding issues in geolocation, IETF (Internet Engineering Task Force) developed Geopriv architecture [5]. According to RFC 3693, there are four significant entities:

- Location Generator: The Location Target collects the location of the end user as well as the location object determines the location. This information is passed to the location server [6].
- Location Server: This is a place where the rules are made and applied to location objects. It receives the publications from the Location Generator as well as the subscriptions from the local recipients.
- Location Recipient: It receives the notifications of the location object from the Location Servers.
- Rule Holder: It has the privacy rules that are used for obtaining, sorting and for the distribution of the location objects for the targets. Transformation of the rules may be made from Rule Holder to the Location Server [6].

Users do not have the ability of efficiently monitoring the settings of their own location revelation in such a scenario, and as a result, they stop having the control when they accept to share the location. Because of this, many users want to remain anonymous and avoid being identified by providers of LBS (Location Based Services) when the data specifically disclose the location of the user [7, 2].

Usually, Apple iPhone Operating System is recognized as a very closed platform. Not like Android phones, Windows platforms, and BlackBerry phones where, before installing, an application is needed to declare the necessary application rights for end-user examination and agreement, iPhone applications can access to everything on the phone by default and the OS gives a warning to users only when its location is accessed by the application. The end-user options are presented by the Android and Windows, while Apple favors the OS to make the decision on device permission during the installation process [7, 2].

There are a few ways to protect geoprivacy when personal data are at stake. One way is to bring strict and detailed government regulations. The purpose is to ensure the rights and privacy of an individual properly safeguarded [8]. Legislation that takes to protect individual privacy, may obstruct the non-intrusive and socially desirable use of georeferenced data. Privacy of geolocation can also be protected using standard protocol – GeoPriv, which describes how to securely collect and transmit

location-information about a target for LBS at the same time it protects the privacy of the individuals that are involved.

Other than forced government rules, statistical methods are there, which is known as statistical masking. A geographical mask is a procedure of changing or hiding the original location of point. Masking the data set, will specify that one will be able to protect the entities which points to the access to data set [2]. These conventional methods do not seek to protect individual level and they do not aim to prevent locational or geographical information from being released or linked to individual attributes [8].

The Geolocation policies are available for the users to accept and to provide their details when and where it is required. The policies are used for routing the traffic based on the location of the users using the applications. The privacy policies are used for specifying the privacy practices that are followed in an organization which states what sort of information will be collected and how the information will be used. The policies are created and defined in terms of the privacy regulations that are created already.

A privacy policy is needed for any organization who gathers, utilizes, reveals, and handles a customer or client's data. A Privacy Policy is a mandatory document which is required by the disclose while dealing with user's personal information. It is a great way to show users that organization can be trusted. It ensures users that organization have procedures in place to handle their personal information with care. The proposed template can help professionals to develop a privacy policies and privacy impact assessments for their services.

3. TEMPLATE DEVELOPMENT

3.1 Methodology

To address the privacy issues, present in the use of Geolocation monitoring tools, this research proposes a set of policies that can be applied to the organization. To serve this purpose a template of policies will be created from reviewing existing Geolocation monitoring policies and identifying the common elements amongst them. The policy will be built with detailed consideration on the compliance with the law with a list of clauses to categorize the policies and integrations of policies based on the data collected, stored, and used. The template can be used by professionals, where personal information of users is stored and used for different purposes.

3.2 Structure of the Template

3.2.1 Introduction

- Purpose:
    - The introduction clause gives a brief overview of what the reader will find in the policy. Key information such as scope of the policy, laws complied indicates that organization takes their users privacy as a serious matter.
- What to include:
    - Briefly explain the purpose of the privacy policy here, including:
    - State the date of publishing or updating of the privacy policy.
    - Summary of what can be found.
    - The scope of the policy
    - Clearly mentioned laws which the organization complies to.
    - Defined keywords or acronyms that is used in the policy.

3.2.2 Description of the organization

- Purpose:
    - This clause details the organization's mission and business objectives. It is advisable provide details on how and whom to contact in case a user has concerns or questions regarding the policy.
- What to include:
    - Identify the organization name, its mission and reason behind collecting personal information.
    - Identify the person or team behind making the policy and guide briefly guide on how to contact the organization in case of queries.

3.2.3 Types of Data collection

- Purpose:
    - Data collection clause makes it clear to a user which type of information organization needs to function correctly and permits users to decide whether they are willing to share that information with the organization.
    - This clause can save the organization from potential liabilities as the organization is forthright about information that they collect. Which eliminates a possibility of a claim of wrongful data collection.
    - Best practice is to describe the type of information collected in simple words. For example, username, email address, IP address etc. However, this can work against the organization if the list is not complete.
- What to include:
    - Identify the types of personal information that the organization collects and stores.

3.2.4 How the data is collected

- Purpose:

- This clause describes all the sources and ways an organization collects data from. Even if the organization only uses and collects data that is directly provided by the user, a provision describing that process is helpful.

- What to include:
  - Clearly state the source of personal information. E.g., a form, survey, cookies, sign-up etc.

3.2.5 Disclosure

- Purpose:
  - This clause is used to specify any scenario in which organization might disclose the non-public (private) information to government bodies or public without consent.
- What to include:
  - Identify any scenarios in which organization might disclose user's personal information to public or government bodies.
  - Clearly specify if the organization discloses personal information without consent in any scenarios.

3.2.6 Data usage & Processing

- Purpose:
  - This clause explains why the organization collects personal information and what does it do with it. Depending on the business an organization can have several purposes for gathering data from users.
  - This phrase should be worded in great depth since no organization wants to be accused of improperly utilizing personal information.
  - The most important aspect of any privacy policy is a clear explanation of how the website/application owner may use the information and whether that use includes or may involve sharing it with others.
  - The goal is to make users trust the organization with their data and show that their nonpublic information will not be disclosed and have been secured in both transit and in databases.
- What to include:
  - Describe all the ways in which the organization uses and processes the collected data.
  - Explain if data will be transferred to other countries outside of user's home country, with the safeguards that organization uses to secure data in transit.
  - List countries that may receive/process the data and for what purpose.
  - Define any steps taken that will ensure the data is processed according to this privacy policy and the applicable law(s) of the country in which the data is located.

3.2.7 Legal basis of processing

- Purpose:
  - It is important that an organization complies with laws in the country they operate and to the country, the organization takes private information from.
  - For example, it is necessary to comply with GDPR if the organization collects data from European residents.
  - If the organization's website targets children under the age of 13, it is subject to the Children's Online Privacy Protection Act (COPPA). Hence the organization needs to meet those rules and disclose it in the privacy policy.
- What to include:
  - State all the laws that organization complies to.
  - List countries, high-level data category, and purpose of collection.
  - Provide information on relevant regulations and how the data is protected in all those jurisdictions.

3.2.8 Specific Data use

- Purpose:
  - Specific use of data clause tells a user why and how their data is being used for. It protects organization from potential liabilities as well.
- What to include
  - Include all uses of data, along with purpose and legal basis of processing.
  - Outline other uses of personal data that may be performed without users' consent (e.g., when anonymized or when legally required).

3.2.9 How long data is stored for.

- Purpose:
  - Many privacy laws such as GDPR requires not to store user's private information more than the time, the data is needed for.
- What to include:
  - Outline all data retention requirements.
  - Justify the duration for data storage.
  - Add a link to a retention schedule if needed.

3.2.10 How data is protected

- Purpose:
    - This clause will let users know that how organization is protecting user's data and what implementations are there to follow for organization in a case of data loss.

- What to include:
    - Describe security measures and controls that are implemented for data security. Consider the following:
    - How to protect against accidental loss, misuse, unauthorized access, modification, and disclosure.
    - How to provide business continuity and disaster recovery.
    - How to train employees on proper data security.
    - How to conduct privacy impact assessments in accordance with laws and regulations.
    - All controls implemented to protect personal data.

3.2.11 Use of Cookies

- Purpose:
    - This clause will let users know that organization uses cookies and other technologies to track them and will have a link to read the cookie policy.
    - This clause also tells users on how to manage their cookie data and how to refuse organization from creating cookies on their browsers.
- What to include:
    - Mention if cookies or similar tracking technologies are used, why they are used.
    - Develop separate cookie policy to define what type of cookies and techniques are used and how to manage them.
    - Any EU-based firm or any foreign company dealing with EU citizens must comply with the EU Cookies Directive.

3.2.12 Business Transfer

- Purpose:
    - Organizations can protect themselves from liability by adding this clause and offer some reassurance for users to continue the consent for the private information given.
    - Even if organization does not anticipate selling or merging the organization, having this clause makes future processes easier if ever organization favors selling as market changes very quickly.
- What to include:
    - Define what happens to the user's private information if organization's business merges with other organization or gets acquired by another larger organization.
    - merely state that users' data will be safeguarded in the same way as it was previously under the prior Privacy Policy.

3.2.13 User's rights regarding personal data

- Purpose:
    - This clause explains what rights users have concerning their information used by the organization.
- What to include:
    - Outline users' rights and describe how users can access and manage their personal data, as required by your regulatory obligations.

3.2.14 Contact Information

- Purpose:
    - This clause informs consumers about how to obtain answers to inquiries concerning their personal information privacy.
    - It is important to give correct information here. If user won't be able to contact the organization they might go directly for the legal take.
- What to include:
    - Explain how a user can reach out to the organization for any questions, concerns, or requests.
    - Provide Phone number, email address and mail address to contact.

3.2.15 Changes to privacy policy

- Purpose:
    - It is important to announce any changes to the privacy policy to users. The method for notification can be defined in this clause.
- What to include
    - Mention the date policy was last updated at.
    - Explain the ways users can get informed about the privacy changes.

3.3 Application 1 – Same IP Report

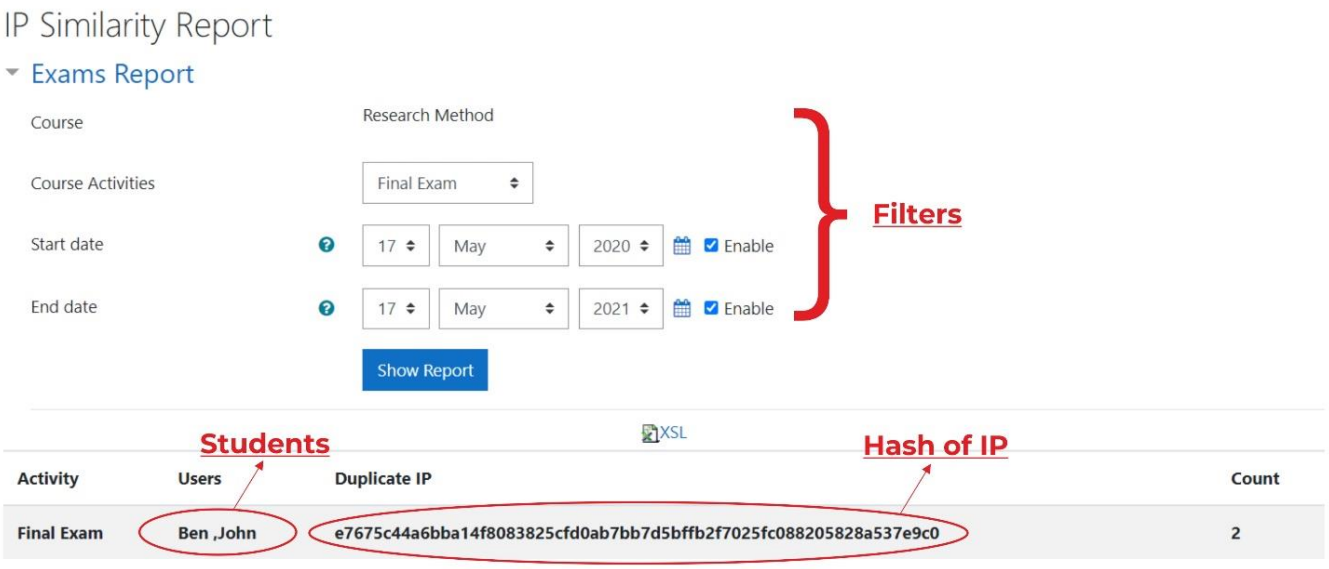

Figure 1: IP similarity report

- The report shows which students used the same IP address to access Moodle modules.
- Filter through options such as modules and dates. For the privacy reasons, the report shows scrambled/ hashed IP address.
- Purpose: In a Moodle-based online quiz/test, to catch the risk of academic dishonesty.
- Workings: The report searches Moodle logs for fields containing the same IP address used by several students for a given module. Filters the date to produce accurate results.
- Users' activities are saved in Moodle's database as log stores. This information comprises the action performed, the IP address, the origin of the IP address, the date, and the username. The same data is used in this report to discover IP addresses that have been logged with various users in the same activity.
- Code Available in link below.
- https://github.com/CyberJedi42/Moodle_code
- Policy: Sample policy based on the developed template is provided in Appendix B.

3.4 Application 2 – On-campus tracking

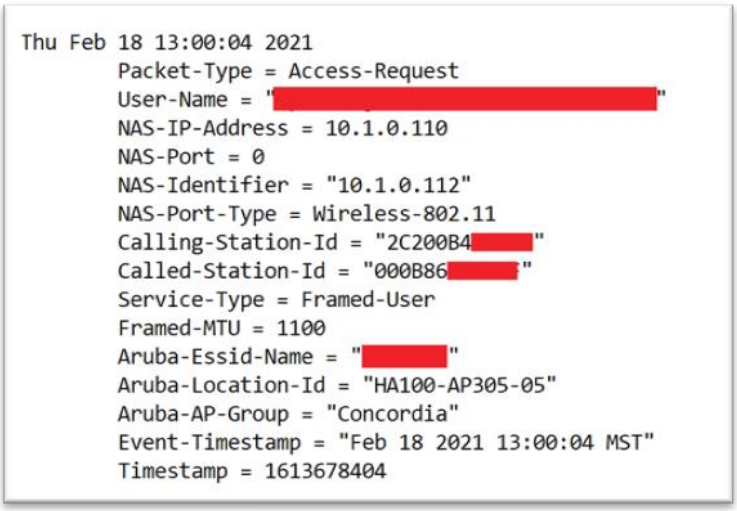

Figure 2:On – campus tracking log

Figure 3: On - campus tracking map

- On-campus tracking is done on users who are connected to campus's WIFI. This will help in notifying people who were in close contact to Covid positive patient. This is done by analyzing the logs collected from campus Wi-Fi and drawing the path of their visit on a map. The aim is to give more specific data on the epidemic, neighborhood-by-neighborhood, to help 'remove the curve' or to disperse the number of COVID-19 cases across extended periods, so that hospitals are not overburdened.
- Data: The logs collect various kinds of information. Some of them include IP address, Email address, Location id, timestamp etc. The data collection of any student takes place through the Wi-Fi logs. The devices connected to the Wi-Fi logs are used for tracing the
- Route of any student. When a device connects to the Wi-Fi, details are automatically connected and placed into the Wi-Fi logs present on the internal server of the organization.
- Policy: Sample policy based on the developed template is provided in Appendix C.

3.5 Policy Review

A privacy policy should be in place for every firm or organization that gathers information about its customers or users. The table given below provides a brief differentiation of the policies mentioned in the template with that of the policies mentioned in the various other organizations. There is an examination of various firms that employ privacy policies to assist someone better understand and compare the policies, as well as to give some direction to organizations seeking to design their own policies. For each firm, a summary of the policies included in the template is supplied.

The template in this document includes clauses such as Description of the Organization, Types of data collected, How the data is collected, Disclosure, Data usage and processing, Legal basis if processing, specific data use, how long the data is stored, how the data is protected, use of cookies, business transfer and user rights regarding their data. The clauses mentioned above are included in the template. From the table, some companies may or may not have the mentioned policies. Some clauses are common to a particular set of companies whereas on the other hand some clauses are not included in that organization.

Terms used in the table:

The column describes various clauses present in the template based on which policies were reviewed.

Yes – Policy had all the necessary information within the clause.

P – Policy had partial information within the clause.

No –Policy did not mention the clause at all and had no information regarding it elsewhere in the policy statement.

No.	Description of organization	Types of Data Collect	How the data is collected	Disclosure	Data Usage & Processing	Legal Basis of Processing	Specific Data Use	How Long Data Is Stored For	How Data Is Protected	Use of Cookies	Business transfer	Users Rights regarding their data
(1)	*P*	*Yes*	*Yes*	*Yes*	*P*	*P*	*Yes*	*No*	*Yes*	*Yes*	*No*	*No*
(2)	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*Yes*	*Yes*
(3)	*Yes*	*Yes*	*P*	*No*	*Yes*	*Yes*	*No*	*Yes*	*No*	*Yes*	*No*	*P*
(4)	*No*	*Yes*	*P*	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*P*	*P*	*Yes*	*P*
(5)	*P*	*Yes*	*Yes*	*No*	*P*	*Yes*	*No*	*No*	*No*	*Yes*	*Yes*	*No*
(6)	*No*	*Yes*	*Yes*	*Yes*	*P*	*Yes*	*No*	*No*	*Yes*	*Yes*	*Yes*	*Yes*
(7)	*Yes*	*No*	*Yes*	*Yes*	*Yes*	*Yes*	*P*	*Yes*	*Yes*	*No*	*No*	*Yes*
(8)	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*P*	*Yes*	*No*	*Yes*	*Yes*	*No*	*Yes*
(9)	*Yes*	*Yes*	*Yes*	*Yes*	*P*	*Yes*	*P*	*No*	*No*	*Yes*	*Yes*	*No*
(10)	*Yes*	*No*	*P*	*Yes*	*No*	*P*	*No*	*P*	*No*	*No*	*No*	*P*

1) University of Alberta (*https://www.library.ualberta.ca/about-us/policies/privacy-policy*)
2) Emerson College (https://www.emerson.edu/policies/privacy)
3) University of Alabama (*https://www.uab.edu/privacy/statements*
4) GAIA GPS (*https://www.gaiagps.com/company/privacy/*)
5) Location Smart (https://www.locationsmart.com/privacy-policy)
6) Geoloqi (http://geoloqi.com/privacy/)
7) University of Toronto (https://www.provost.utoronto.ca/wp-content/uploads/sites/155/2018/06/fippa.pdf)
8) Fortinet (https://www.fortinet.com/corporate/about-us/privacy)
9) Dropoff(https://www.dropoff.com/privacy/)
10) Life360 (https://www.life360.com/terms_of_use/, https://www.life360.com/privacy_policy/)

Table 1: Reviewed Policies

.

4. CONCLUSION

Developing a detailed privacy policy is typically oversighted by many organizations when it comes to geolocation tracking services. This leaves the organization vulnerable when legal issues arise and makes user not to trust it is practices. The presented template was derived from observing and comparing many policies and statements. The presented template acknowledges the issues present in current privacy policies and provides a robust structure to ensure that policy includes every essential clause and is clear and direct. 3 sample policies derived from the template, show how much detailed and elaborative a privacy policy needs to be. This template will help IT professionals to develop policies which protects the organization from any liabilities and help an end-user understand how their personal information is being collected, stored, and processed at the organization.

5. REFERENCES

[1] B. Estes, "Geolocation—The Risk and Benefits of a Trending Technology," *Isaca Journal*, vol. 5, pp. 1-6, 2016.

[2] S. Gray, "A CLOSER LOOK AT LOCATION DATA: PRIVACY AND PANDEMICS," 17 December 2020.

[Online]. Available: https://fpf.org/blog/a-closer-look-at-location-data-privacy-and-pandemics/.

[3] O, Nicole, "10 Common Issues with Privacy Policies," privacypolicies, 05 January 2021. [Online]. Available: https://www.privacypolicies.com/blog/privacy-policy-common-issues/.

[4] G. Beall, "10 Ways to Keep Your Information Safe in The Digital Age," 15 October 2018. [Online]. Available: https://www.business2community.com/cybersecurity/10-ways-to-keep-your-information-safe-in-the-digital-age-02130163.

[5] P. Podiyan, S. Butakov and P. Zavarsky, "Study of compliance of the Android location APIs with Geopriv".

[6] A. Cooper and T. Hardie, "GEOPRIV: Creating Building Blocks for Managing Location Privacy on the Internet," 7 September 2009. [Online]. Available: https://www.ietfjournal.org/geopriv-creating-building-blocks-for-managing-location-privacy-on-the-internet/.

[7] H. Cheug, M. Elkhodr and S. Shahrestani, "A review of mobile location privacy in the Internet of Things," 2012 Tenth International Conference on ICT and Knowledge Engineering, 2012.

[8] M. Kwan, "Protection of Geoprivacy and Accuracy of Spatial Information: How Effective Are," 2014.

[9] R. Azmi, K. Win, W. Tibben,"*Review of cybersecurity frameworks: context and shared"* , no. Sciences: paper part B, p. 38, 2018.

[10] Z. Hang, L. Jorge, A. Roy and S. M. Bellovin, "https://www.cs.columbia.edu," [Online]. Available: https://www.cs.columbia.edu/~smb/papers/rofl-refine.pdf. [Accessed 06 2021].

[11] H. Schulzrinne, H. Tschofenig, J. Polk, J. Morris and M. Thomson, "https://www.hjp.at/," January 2013. [Online]. Available: https://www.hjp.at/doc/rfc/rfc6772.html. [Accessed 06 2021].

[12] M. Jocelyn, "Clauses for Privacy Policy," 22 December 2020. [Online]. Available: https://www.termsfeed.com/blog/privacy-policy-clauses/.

[13] B. Donnet, M. kaafar, Ingmar Poese, "IP Geolocation Databases: Unreliable?," 2011. [Online]. Available: https://www.depositonce.tu-berlin.de/bitstream/11303/11340/1/tr_2011-03.pdf.

[14] E. Katz-Bassett, J. John P, A. Krishnamurthy, D. Wetherall, T. Anderson and Y. Chawathe, "Towards IP Geolocation Using Delay and Topology," [Online]. Available: https://cs.gmu.edu/~iyoun/geo/pdf/katzbassett.pdf.

[15] S. ZU, X. LUO, S. LIU, Y. LIU and F. LIU, "City-Level IP Geolocation Algorithm Based on PoP Network Topology," 29 October 2018. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8513753.

[16] Z. Dong, R. Perera, R. Chandramouli and K. Subbalakshmi, "Network measurement based modeling and optimization for IP geolocation," 3 August 2011. [Online]. Available: http://iris.nyit.edu/~zdong02/publications/DongIPgeo11.pdf.

[17] Z. Hu, J. Heidemann and Y. Pradkin, "Towards Geolocation of Millions of IP Addresses∗," [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.739.4656&rep=rep1&type=pdf.

[18] C. Jensen, P. Potts, "Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices," [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.629.1633&rep=rep1&type=pdf.

6. APPENDIX

6.1 Appendix A: Template

6.1.1 INTRODUCTION

The privacy notice is used to disclose the organization's privacy policies in accordance with privacy regulations such as the General Data Protection Regulation (GDPR). We want to assist you realize what personal information we gather, how it is used by us, as well as how much authority you have over that. This Privacy Policy applies to the organization's website as well as any features and online or offline services offered by the organization that include a link to this Privacy Policy. User should read the privacy policy and agree to the services being provided by the organization, by accepting the terms and conditions the user allows the organization to collect and use their personal information. The following data may be included in this privacy notice:

1. What personal information is gathered through the website?
2. The way personal information is gathered, utilized, shared, kept, and or else processed.
3. The security processes put in place to secure your information.
4. Your options and privileges in relation of how your data is used.
5. How to get in touch with us for matters such as correcting mistakes in your data or requesting the deletion of your personal data.

Please read the following privacy notice to learn about the processing, collecting, sharing, and protection of your personal data, as well as your rights.

6.1.2 WHO WE ARE?

[Organization] belongs to the [describe kind of organization] category. Our aim is to [briefly state organization purpose], and in order to do so, we gather and use personal information that you provide.

6.1.3 DATA WE COLLECT

We have access to whatever information you supply to us. The information we collect may include the following type of data:

- [Full name]
- [Email address]
- [Username]
- [Phone number]
- [Address]
- [Date of birth]
- [Information about any complaints, enquiries, and communication you make with us]
- [Details on services received from us]
- [Location]
- [Photos]
- [Browser information and settings]
- [Mailing address]
- [Other…]

Specify which, if any, data is collected from third parties, including the type of data and source.

6.1.4 HOW THE DATA IS COLLECTED

[Organization] may collect the personal information from you through various modes of means. This can include data through the surveys, google forms, cookies or upon signing up any application that you are trying to access.

6.1.5 DISCLOSURE

Except where we think it is essential for the performance of our company or when publication is obliged by legislation, [Organization] does not quite release any non-public personal details concerning our clients or former clients to anybody. We shall not make any releases of non-public private details to other firms that may wish to promote products and services to you without your agreement, save in those specified, restricted circumstances.

6.1.6 HOW DO WE UTILIZE YOUR DATA

Your private data and information might be utilized for the following purposes.

- Professional working of the company.
- Content and user experience customization
- Account Creation
- Research and Development
- Respond to your inquiries and suggestions.
- Forming a contract with the company
- Content and user experience tailor made.
- When you use [website], you must identify yourself.
- Account creation and management.
- Organizing polls, surveys, and competitions.
- Internal research and development.
- Legal responsibilities
- Internal reviews are performed.
- Duties specified in any contracts with clients are met.
- Collecting comments and thoughts on the services we offer.
- Reporting of updates to our services to customers.
- Respond to your inquiries and suggestions.
- Manage your purchases.

[Other…]

Clearly mention any other use of private information performed by the organization.

.

6.1.7 LEGAL BASIS OF PROCESSING

We analyze private information in order to pursue our legitimate purposes, as long as such interests, rights, or freedoms do not contradict with those of our users. Marketing, research, and corporate development methods are examples of legal business

interests. We may use your private information for other reasons with your approval, but you have the option to revoke your consent at any point and for any reason.

PIPEDA:

In general, PIPEDA aims to find the right balance between people' right to privacy in their personal information and organizations' need to gather, utilize, or share personal information in the context of doing business. PIPEDA imposes a set of legal constraints on businesses based on the 10 principles listed below:

- Accountability
- Identifying purposes
- Consent
- Limiting collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance

Under PIPEDA, organizations may only gather, utilize, or disclosure of personal data for reasons that a legit person would ponder fit in the circumstances.

GDPR – The GDPR defines six legal grounds that must be justified to warrant relevant conditions for data processing:

- Consent
- Contract
- Legitimate interests
- Vital interests
- Public tasks
- Legal obligation

Provide additional context to each relevant legal basis, such as if the legal basis is "legitimate interest," what is that interest? If the legal basis is "consent," define the right to withdrawal consent.

COPPA - The Children's Online Privacy Protection Act need to be complied if children fall under the market value of organization. This includes children aged 13 or below.

US Privacy Laws – US does not central federal level privacy law however has multiple vertically privacy focused laws. This includes US Privacy Act of 1974, HIPAA and GLBA.

US State Privacy laws – Multiple states of US has defined their own laws to protect their consumers. Main three states are California, Nevada, and Virginia. If your organization collect and processes data from these states, you must comply with their privacy laws.

We have put in place security rules and regulations to guarantee that data in these jurisdictions is properly safeguarded [e.g., contractual obligations, data transfer agreements].

6.1.8 SPECIFIC DATA USE

To have full access to the application, you may register for an account. Information such as your name and email address are collected throughout this procedure. This data is used to contact you and offer you with products and services that are pertinent to you. When necessary or permitted by law, personal data could be used without the user's knowledge or consent. We may require your location of the data if required by the services of the company. Information regarding the number of times the applications are visited are send to the us to keep a track. Cookies may be used along with other tracking mechanisms to keep a track of your activities.

Private details would be used even without knowledge of the user or agreement in cases where it is necessary or authorized by law, or where it has been anonymized or pseudonymized so that it can no longer be linked to the user. It implies we have eliminated personally identifiable information from the data we are left with, making it impossible to link it to you as a person.

6.1.9 HOW LONG WE STORE YOUR DATA

We may store your personal data for till it is required for the reasons for which it was collected. We will only preserve personal information for as long as it is necessary to fulfil the purposes for which it was collected. If it is largely for public interest recordkeeping or statistical reasons, personal information may be retained for longer durations. The data will not be stored for a time longer than the period of time you have an account with us unless and until mentioned and obligatory by the law. If the data is not needed, it shall be deleted or removed from the database. If that does not happen, the personal information will be securely stored and isolated.

List any relevant regulations and basic requirements, such as HIPAA, FERPA, or others for data storage.

6.1.10 HOW WE PROTECT YOUR DATA

You should be assured that your personal data will not be shared with any other organization or institution and that the data will be safe and secure with us. We have put in place necessary procedures to prevent unauthorized parties from losing, misusing, accessing, altering, or disclosing personal information. Third party applications are given access to the personal data only on the information that is necessary to them and that is needed by them to accomplish their specific task. All staff must also sign confidentiality agreements and get annual training on how to handle sensitive data.

Procedures for dealing with a possible data leak have already been established and tested. These processes are intended to notify impacted persons and regulators of the breach so that consequences can be minimized.

6.1.11 USE OF COOKIES

Cookies are used for a multitude of reason on [the website]. These "cookies" are little data files that are saved on your hard drive and help us improve your online experience. You will not have to log in with your credential's multiple times from a certain browser

since cookies are often used to recognize you, sparing you time when using our page. We also use cookies to promote products depending on your browsing history, to store and maintain your website settings, to enable content, and to analyse your browsing habits in general. Cookies on the website may be linked to your personal information. For further information, read our [cookie policy].

6.1.12 BUSINESS TRANSFER

Your consent to the University sending your information to the new owner or successor entity if the ownership of our business changes, or if we undertake a corporate organization or any other action or transfer between Concordia University companies. When and where necessary, Concordia University will notify the proper authorities.

6.1.13 YOUR RIGHTS REGARDING YOUR PERSONAL DATA

You have all the rights to know how your data is being used and processed. We strive to keep data accurate and up to date. If your personal information changes (for example, if you move), please tell us and update your information. The following are legal rights that you have:

- Request any data we have on file for you.
- Request that we rectify the personal information we have on file for you.
- When there is no legitimate justification for us to maintain personal data, you may request that it be deleted or erased.
- You have the option to stop interacting with us at any moment.
- Let us know if you have any concerns about the information, we have collected about you.

To exercise these rights, please contact us via the email, mail, or phone information provided below in the “Contact Information” section.

6.1.14 CONTACT INFORMATION

Regarding any questions or queries about the policies you can contact us by email at xyz@organization.com or by phone at +1 (xxx)-(xxxxxxx)

6.1.15 CHANGES TO PRIVACY POLICY

At any moment, we retain the right to make changes to Our Privacy Policy. Any modifications will be communicated to You by publishing the revised Privacy Policy on this page.
Prior to the modification being effective, we shall tell You by email and/or a prominent notice on Our Service, and the "Last updated" date at the top of this Privacy Policy will be changed. It is recommended that you examine this Privacy Policy on a regular basis for any updates. When changes to this Privacy Statement are posted on this website, they become effective.

6.2 Appendix B: Sample Policy

6.2.1 INTRODUCTION

Concordia University of Edmonton is dedicated to safeguard and respect your privacy. This privacy notice (together with our Terms of Service and any other documents linked to in it) describes how we will handle any personal data you provide to us. The application used in this policy is Moodle. It is used for identifying the students using the same IP address. Please read the following carefully to have a better understanding of our views and policies regarding your personal information, as well as how we will manage it.

6.2.2 WHO WE ARE?

CUE is a boutique university, small enough that every student is essential yet large enough for a global outlook. Our mission is that Concordia University of Edmonton is a learning community based on scholarship and academic freedom that prepares students to be independent thinkers, ethical leaders, and community members.

6.2.3 DATA WE COLLECT

We collect your (students) data that includes personal data such as your

- First name
- Last name
- Username
- Email Address
- IP address
- Activities on Moodle

The data collected gives your details and stats. Our university can fulfill the mandate, duties, and obligations as an institution. The information that is collected is necessary to identify and monitor any academic misconducts.

6.2.4 HOW THE DATA IS COLLECTED

We collect your data by means of surveys, google forms as well as the details that you provide while signing into Moodle. We collect the various information such as your name, email address, date of birth, the course that you are enrolled in, year of enrolment. The data that is collected is stored in the database of the university and it is secure.

6.2.5 DISCLOSURE

The university assures you that your personal data will not be disclosed with any third-party organization. The details provided by you will be safe with us and that it will not be shared with anyone outside the university without your consent.

6.2.6 HOW DO WE USE YOUR DATA

Our university uses the data of the students and provides to the application (Moodle) that is used. The data provided by you is used for finding if any academic misconduct takes place between two or more students. This is used in to create a report in Moodle and used to find if the same IP address is being used by the students. The instructor in charge will get to know the hash IP address.

6.2.7 LEGAL BASIS OF PROCESSING

As per the rules and regulations of our university you must abide by the procedures and protocols provided. The student must also accept the rules and regulations of Moodle. You give your organization the access to some information voluntarily. This includes Name, email address, profile photo, physical address, IP address and consent to track your activities on Moodle.

6.2.8 SPECIFIC DATA USE

The data provided by you is used for purposes related to security and not more than that. It is specific and will not be used without the consent of the user. The main purpose is privacy management, which can be achieved by following the rules and regulations of our university and Moodle.

6.2.9 HOW LONG WE USE YOUR DATA

Your personal information is stored with us as long as you are enrolled in a specific course and with Concordia University. On the completion of the course, your data will be stored in a secure database and not used unless and until required by the law. Your data is secure with us and will not be hindered.

6.2.10 HOW WE PROTECT YOUR DATA

Your personal data and information will not be shared with any other organization or institution and secured in a proper and safe database. Upon agreeing with the policies, you should be aware that your data will not be shared to any other third-party organization or any untrusted source. Technical and managerial measures are taken to protect your data securely with us. You should be aware of using and providing your information in a trusted environment.

6.2.11 USE OF COOKIES

We utilize cookies to enhance the performance of our website and services by recording user preferences, tracking user trends, and displaying relevant advertising to you. By continuing to use our site, you consent to use our privacy policy, along with the use of the cookies.

6.2.12 BUSINESS TRANSFER

If any changes take place, or if there is any change in the ownership of the university, or our business, you consent to the university to transfer your information to the new owner so that we continue providing our services. The university will keep you updated of the changes taking place that is applicable to the law.

6.2.13 YOUR RIGHTS REGARDING YOUR PERSONAL DATA

The student and the staff have all rights to review their data, you can ask at any point of time to review your data. The staff have all the rights to access the information of any student. Upon agreement to the policies, the staff can at any point of time gather information such as the student's name, course name, IP address and much more. This makes it easier for them to figure out how many students have performed the activity under the same IP address.

6.2.14 CONTACT INFORMATION

For further details contact xyz@concorida.ab.ca or you can even call us at +1 (xxx)-(xxxxxxx).

6.2.15 CHANGES TO PRIVACY POLICY

The privacy policy was last updated on MM/DD/YYYY

Any changes will be communicated to you by posting the updated Privacy Policy on this page and can also be found on our URL.

6.3 Appendix C: Sample Policy 2

6.3.1 INTRODUCTION

Concordia University of Edmonton is dedicated to safeguard and respect your privacy. This privacy notice (together with our Terms of Service and any other documents linked to in it) describes how we will handle any personal data you provide to us. The application used in this policy is Google Maps. It is used for tracking the users in campus who have been in close contact to Covid positive patient. The data of the patients along with the students and staff of our university is collected and stored in the database. The data that is collected is confidential and is not shared with anyone. It is our aim to collect the data from the students and use the personal data provided by you. Please read the following carefully to have a better understanding of our views and policies regarding your personal information, as well as how we will manage it.

6.3.2 WHO WE ARE?

CUE is a boutique university, small enough that every student is essential yet large enough for a global outlook. Our mission is that Concordia University of Edmonton is a learning community based on scholarship and academic freedom that prepares students to be independent thinkers, ethical leaders, and community members.

6.3.3 DATA WE COLLECT

We collect your data through the Wi-Fi logs. Your devices connected to our Wi-Fi are used for tracing your route that is made in the campus. Your details such as

- IP address
- Email address
- Username
- Packet type
- Wi-Fi access points
- Location ID
- Timestamp
- Device OS type

are then automatically collected when your device connects with the campus Wi-Fi and are placed in the Wi-Fi logs present in the internal server of our campus.

6.3.4 HOW THE DATA IS COLLECTED

We collect your data by means of surveys, google forms as well as the details that you provide. The details are also in regard to that of the google maps. We collect the various information such as your name, email address, date of birth as well as if you have any history of COVID. The data that is collected is stored in the database of the university and it is secure.

6.3.5 DISCLOSURE

The university assures you that your personal data will not be disclosed with any third-party organization. The details provided by you will be safe with us and that it will not be shared with anyone outside the university without your consent.

6.3.6 HOW DO WE USE YOUR DATA?

Our university uses the data of the users and is used along with the Google maps and integrate it with them. The data provided by you if any user has been in a proximity to a covid positive patient. Using Google Maps a route is traced in the campus. The data provided by you is stored in the internal server and used for the purpose of geolocation tracking.

6.3.7 LEGAL BASIS OF PROCESSING

As per the rules and regulations of our university you must abide by the procedures and protocols provided. You must also accept the rules and regulations of Google Maps. You give your organization the access to some information voluntarily. This includes Name, email address, profile photo, physical address, IP address and consent to track your activities through geolocation tracking.

6.3.8 SPECIFIC DATA USE

The data provided by you is used for purposes related to security and not more than that. It is specific and will not be used without your consent. The main purpose is privacy management, which can be achieved by following the rules and regulations of our university and Moodle.

6.3.9 HOW LONG WE USE YOUR DATA

Your personal information is stored with us as long as you are enrolled with Concordia University. On the completion of your course with the University, your data will be stored in a secure database and not used unless and until required by the law. Your data is secure with us and will not be hindered.

6.3.10 HOW WE PROTECT YOUR DATA

Your personal data and information will not be shared with any other organization or institution and is secured in a proper and safe database. Upon agreeing with the policies, you should be aware that your data will not be shared to any other third-party organization or any untrusted source. Technical and managerial measures are taken in order to protect your data securely with us. You should be aware of using and providing your information in a trusted environment.

6.3.11 USE OF COOKIES

We utilize cookies to enhance the performance of our website and services by recording user preferences, tracking user trends, and displaying relevant advertising to you. By continuing to use our site, you consent to use our privacy policy, along with the use of the cookies.

6.3.12 BUSINESS TRANSFER

If any changes take place, or if there is any change in the ownership of the university, or our business, you consent to the university to transfer your information to the new owner so that we continue providing our services. The university will keep you updated of the changes taking place that is applicable to the law.

6.3.13 YOUR RIGHTS REGARDING YOUR PERSONAL DATA

You have all rights to review your data when and where required. You may at any point of time ask us to make any changes in the data. Upon agreement to the policies, our staff can gather information such as your name, course name, IP address and much more. This makes it easier for us to figure out how many users have been in close contact to a covid positive patient and is easier to get a track in campus.

6.3.14 CONTACT INFORMATION

For further details contact xyz@concorida.ab.ca or you can even call us at +1 (xxx)-(xxxxxxx).

6.3.15 CHANGES TO PRIVACY POLICY

The privacy policy was last updated on MM/DD/YYYY

Any changes will be communicated to you by posting the updated Privacy Policy on this page and can also be found on our URL.

About the authors:

To be added after the review