THERE'S A (POT)HOLE IN YOUR PRIVACY POLICY: PRIVACY CONCERNS IN CANADIAN PROBLEM-REPORTING WEBSITES

11/17/2026

Indrani Ray, Professor Maria Wolters, Professor Kami Vaniea







Municipal Problem Reporting (311) Websites

Pothole



Required fields are marked with asterisks (*)

Report a problem

What would you like to report? *

- ○ Graffiti
- ○ Illegal sign
- ○ Litter in a playground, park or trail
- ○ Needles
- ○ Parking complaint
- ○ Property standards complaint
- ◉ Pothole
- ○ Sidewalk snow clearing
- ○ Sidewalk trip hazard
- ○ Trail surface maintenance
- ○ Other

Repaired Pothole

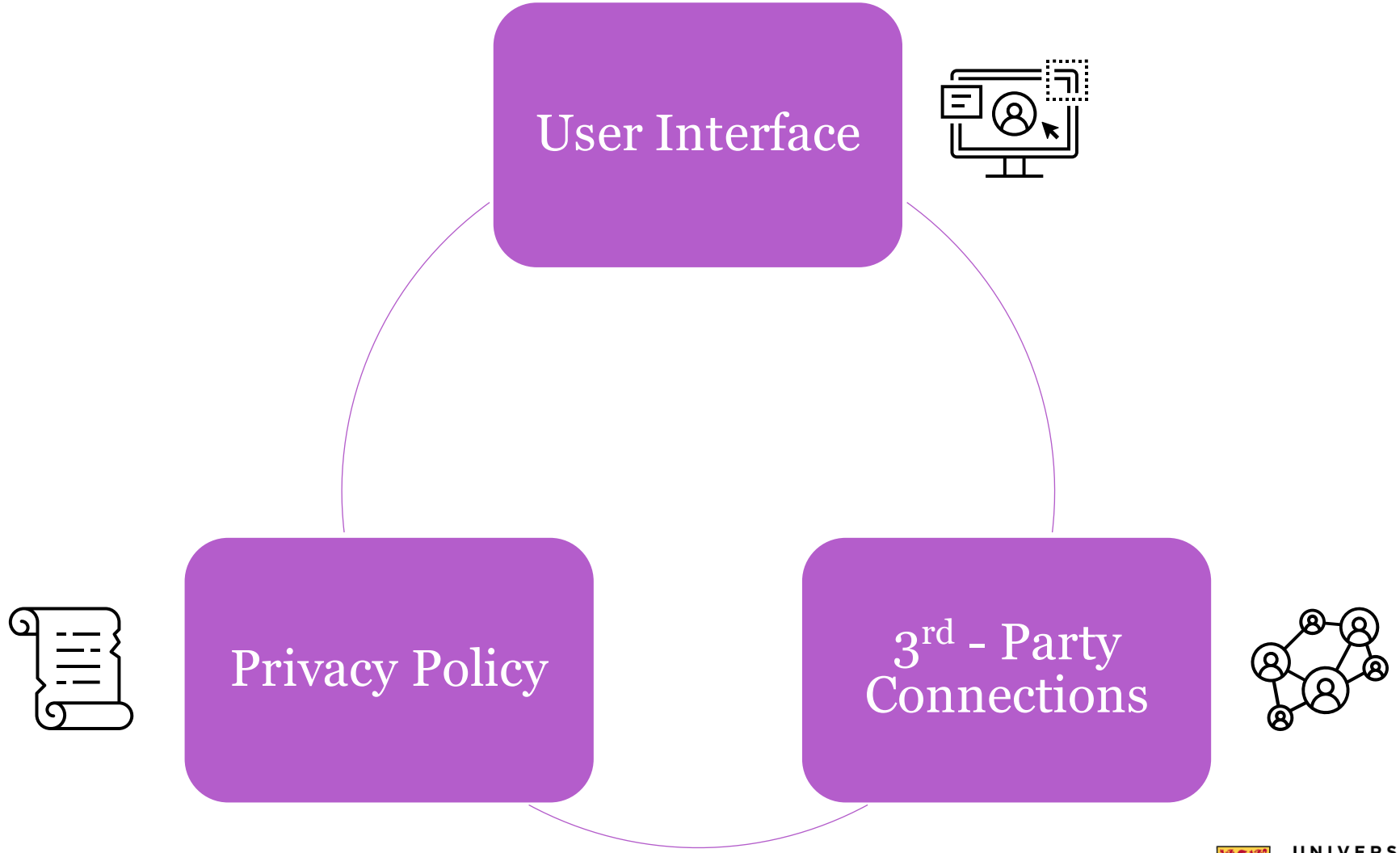


Approach

- E-governance success depends on citizen trust.
- We ask: how are these sites addressing and informing citizens of their data's privacy?

- Inspect 311 websites of 13 Canadian cities
  - Largest city in each Province except Prince Edward Island (no city with 311 website)
- Consider infrastructure-related services
  - E.g., pothole repair, snow removal, tree maintenance, etc.

We Study: Personal Data Collection and Tracking Practices of 311 Websites



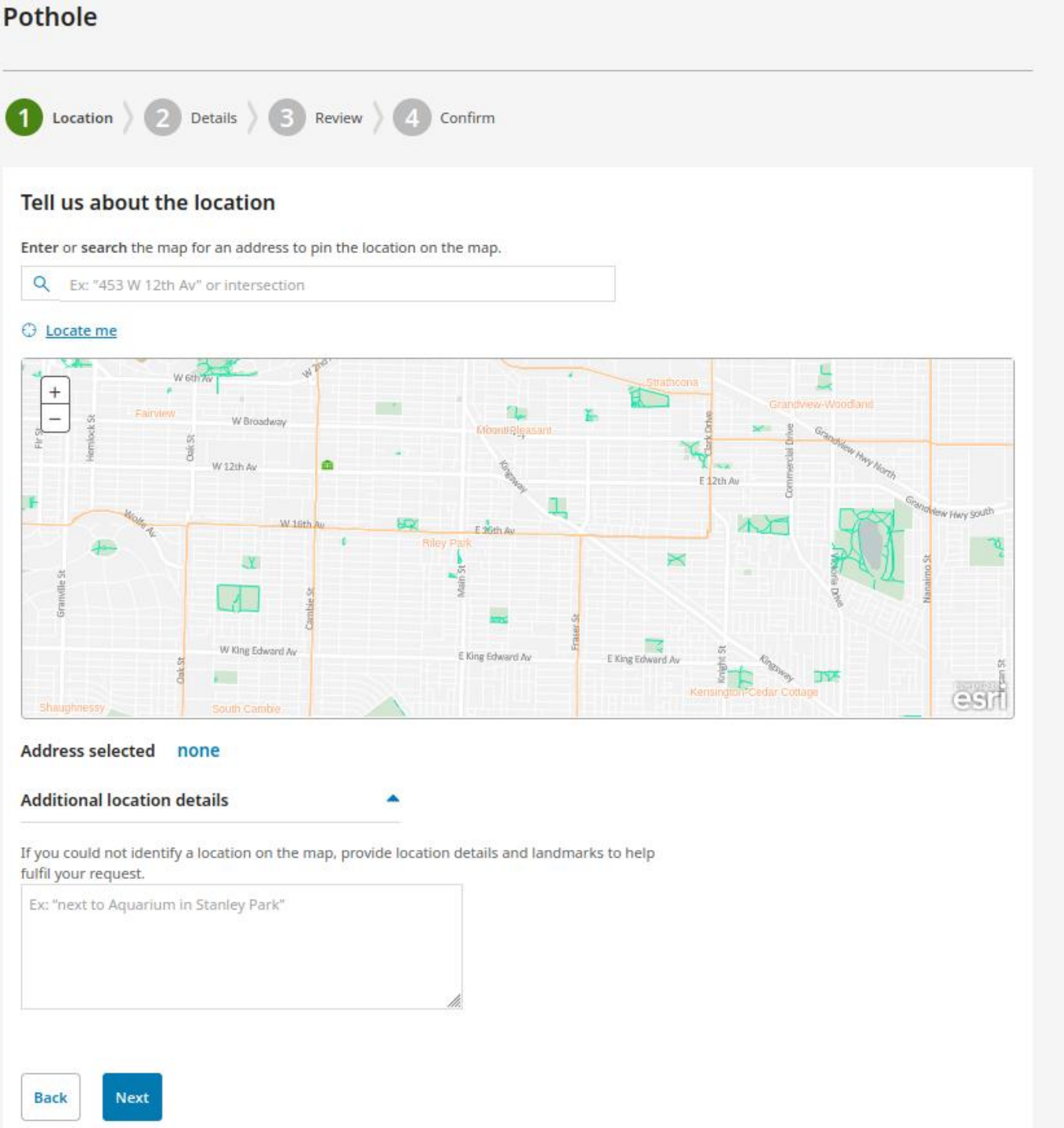
METHODS: USER INTERFACE

What personal data is a user expected to supply when submitting a 311 request?

Example 311 Request

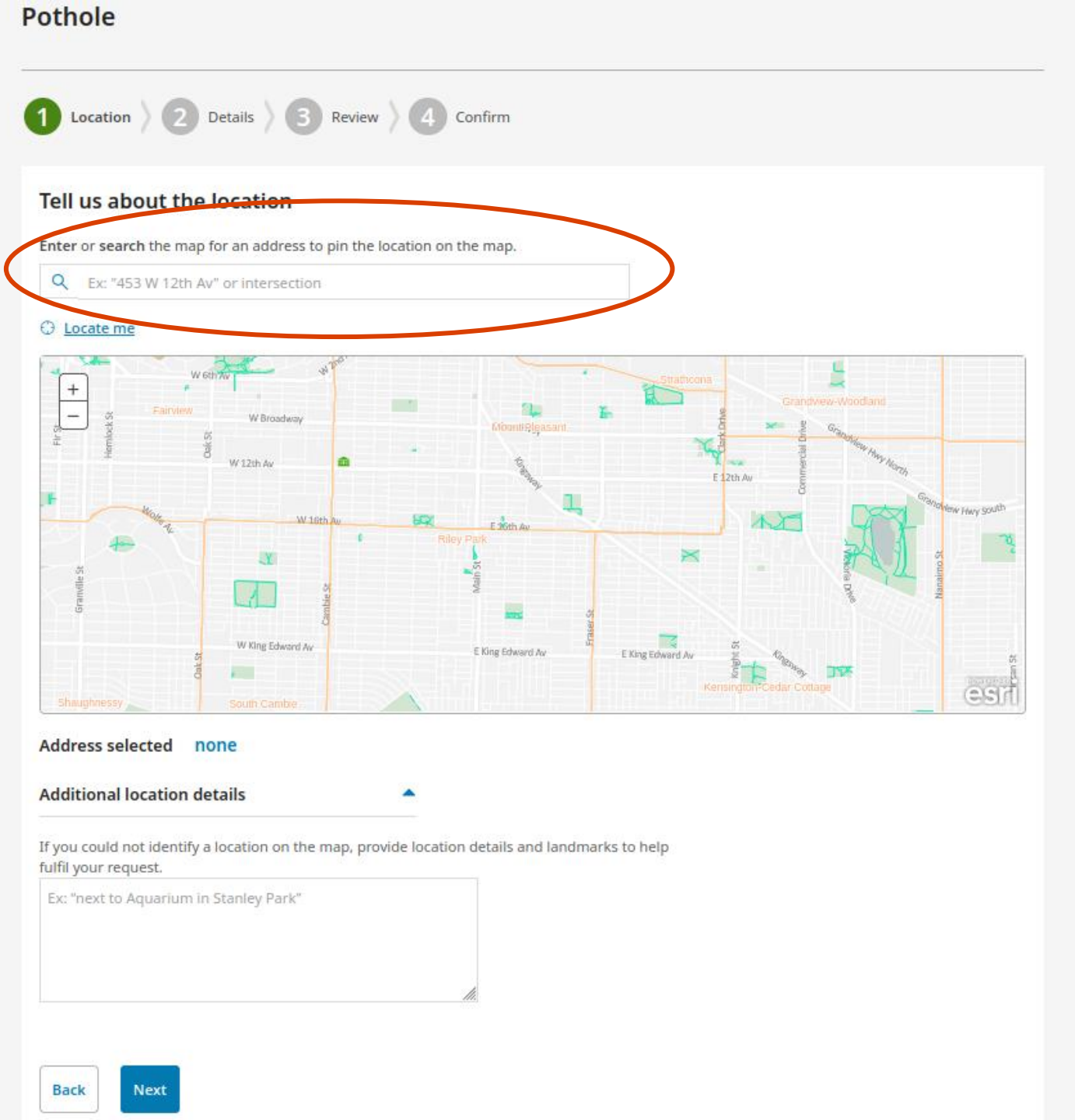
UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

Example 311 Request



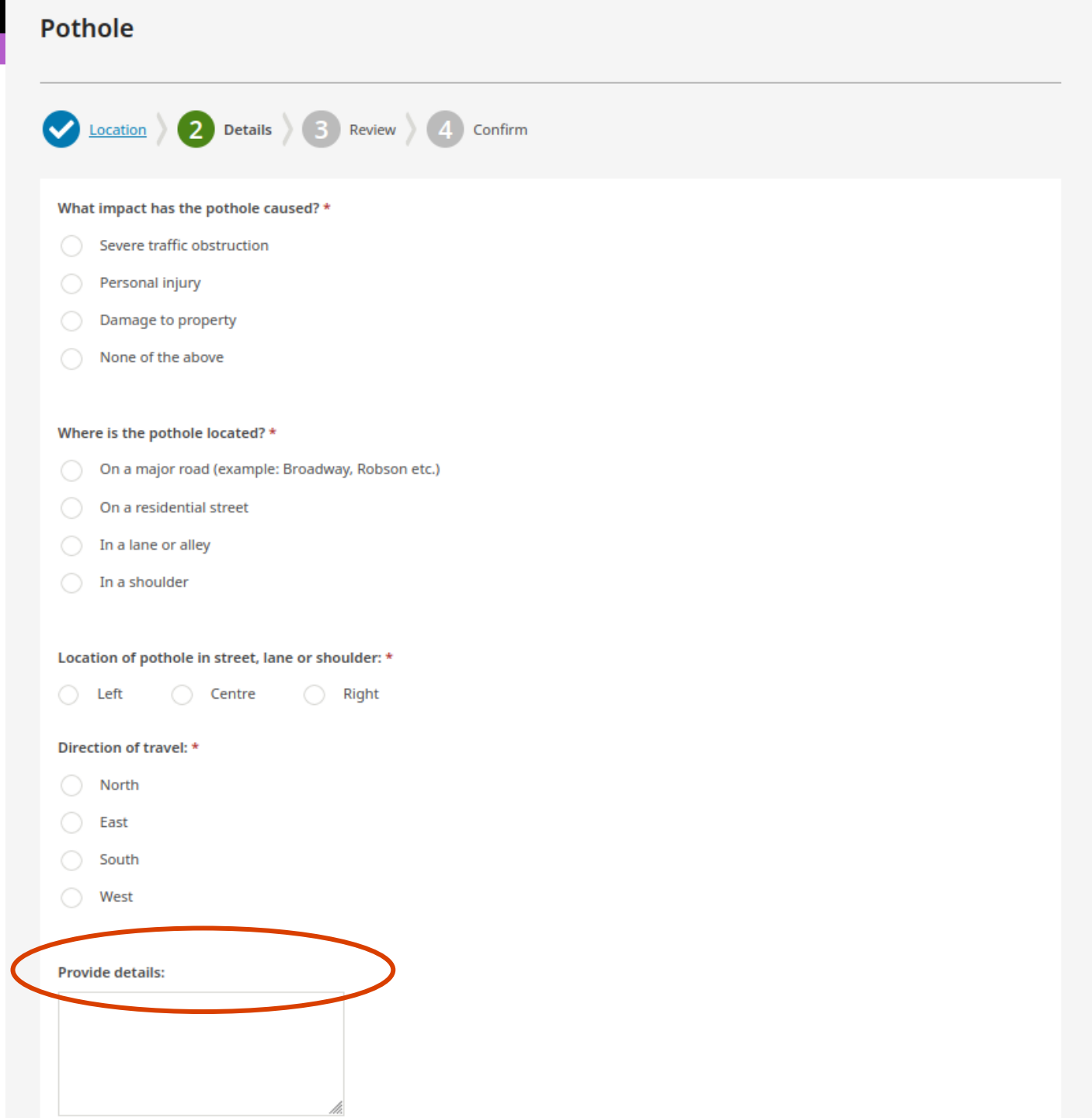
Example 311 Request

- Location



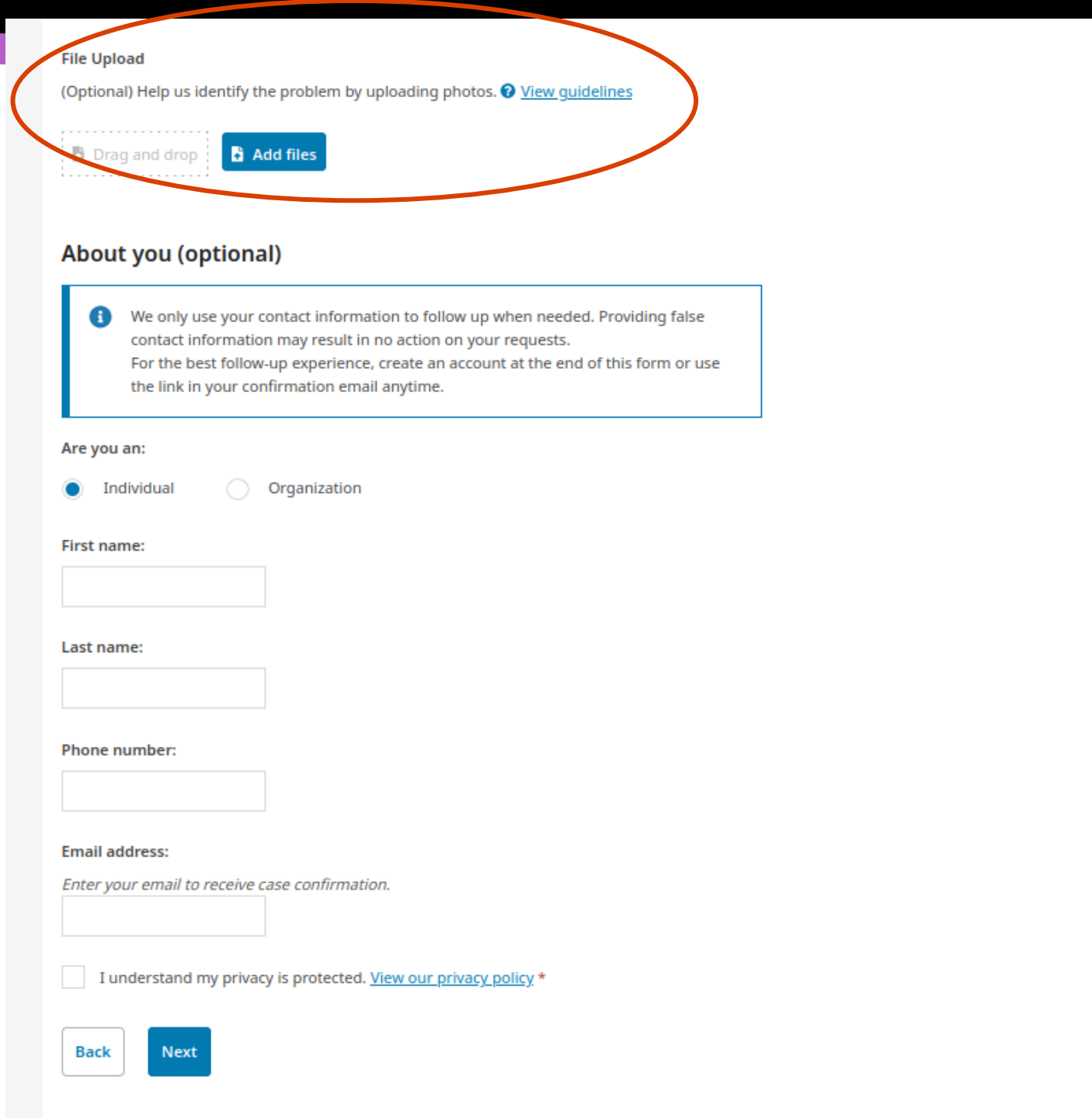
Example 311 Request

- Location
- Details



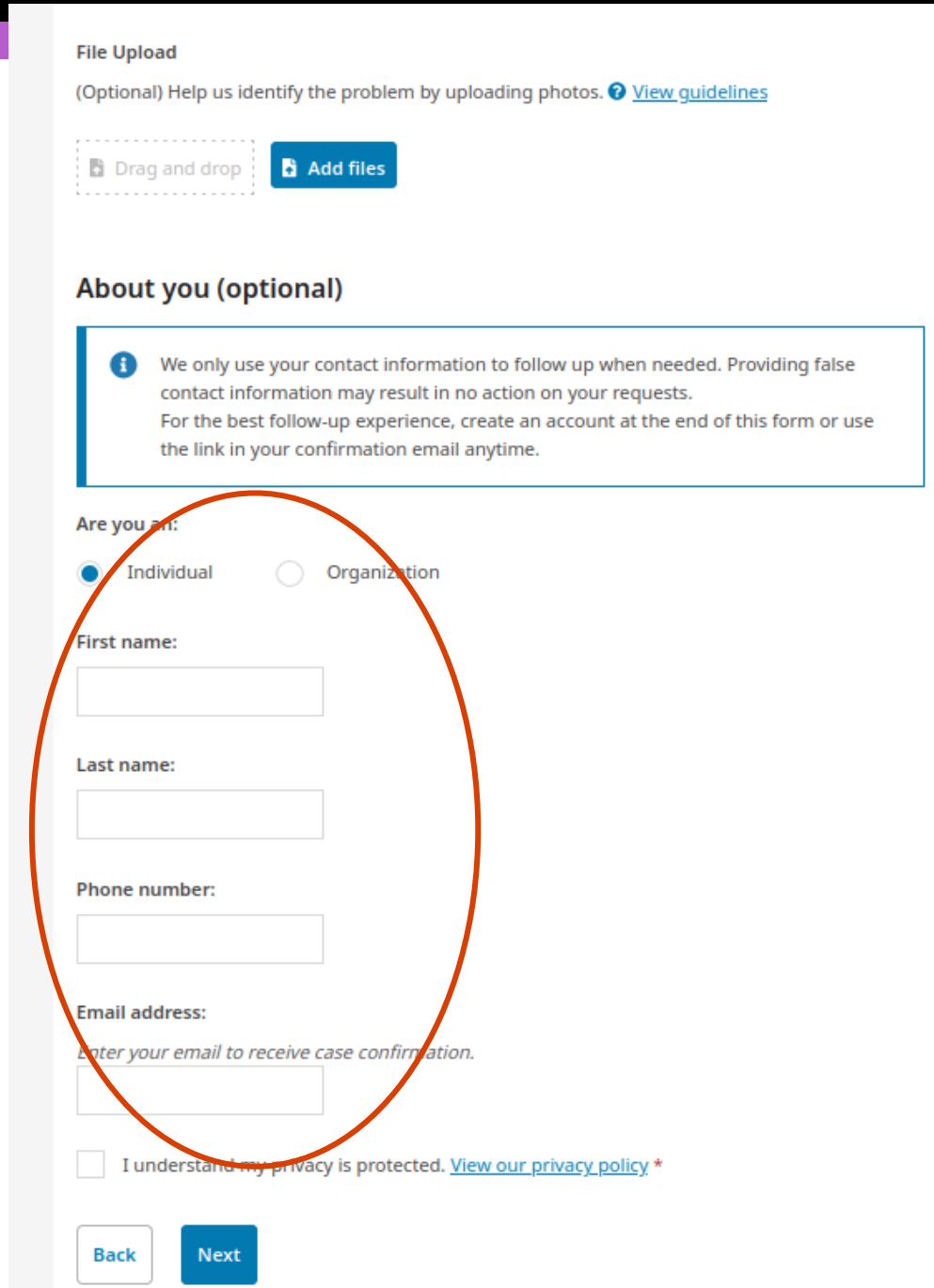
Example 311 Request

- Location
- Details
- Attachment



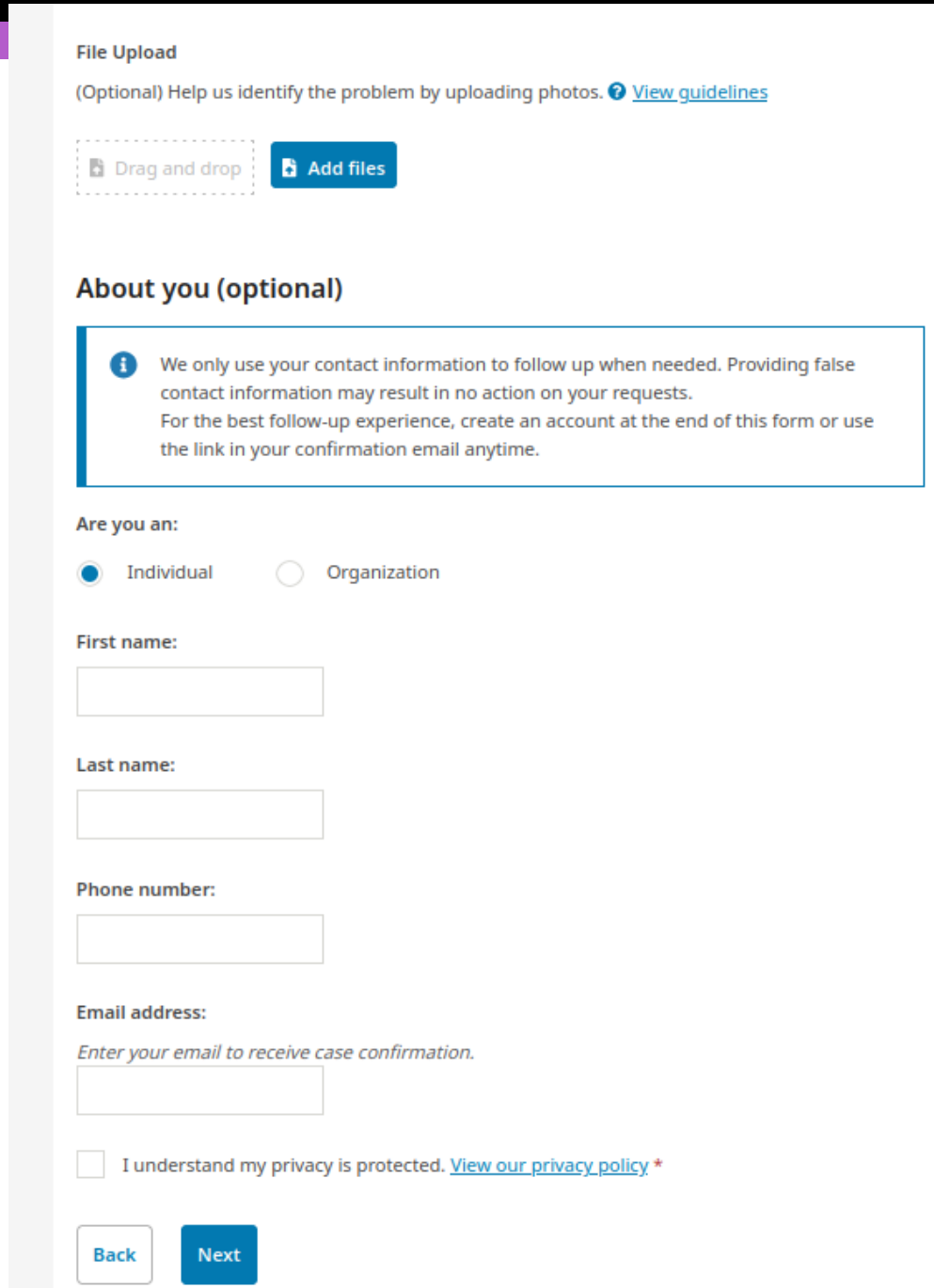
Example 311 Request

- Location
- Details
- Attachment
- First name
- Last name
- Phone
- Email



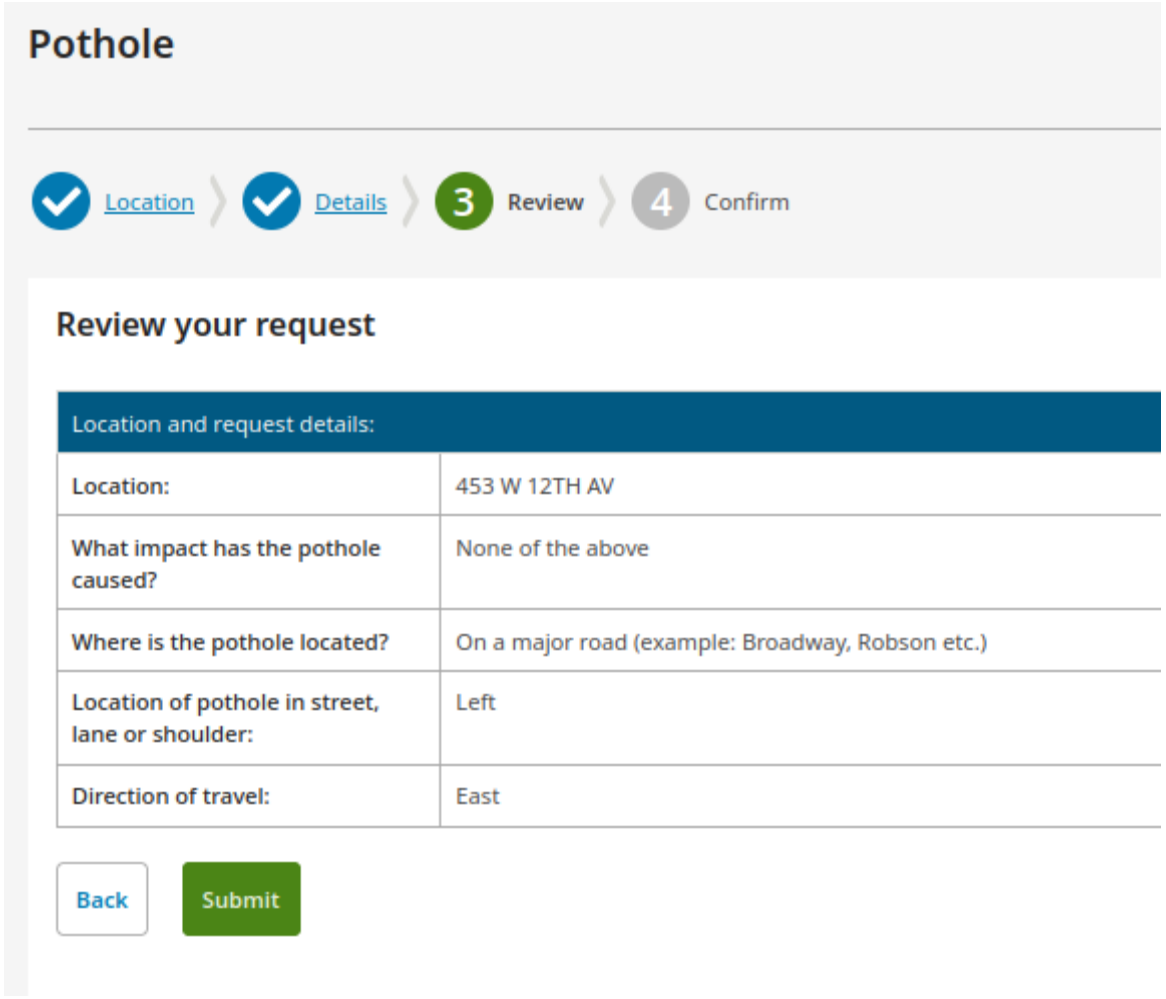
Example 311 Request

- Location
- Details
- Attachment
- First name
- Last name
- Phone
- Email
- Address



Example 311 Request

- Location
- Details
- Attachment
- First name
- Last name
- Phone
- Email
- Address



METHODS:
3RD – PARTY CONNECTIONS

Which third parties are contacted and engaged in tracking?

Third Parties Contacted During Pothole Request

- Record HTTP Archive (HAR) files while reporting a pothole
- Identify known trackers being contacted (based on DuckDuckGo Tracker Radar)
- Analyze cookie, query string, and post data to identify further tracking behavior

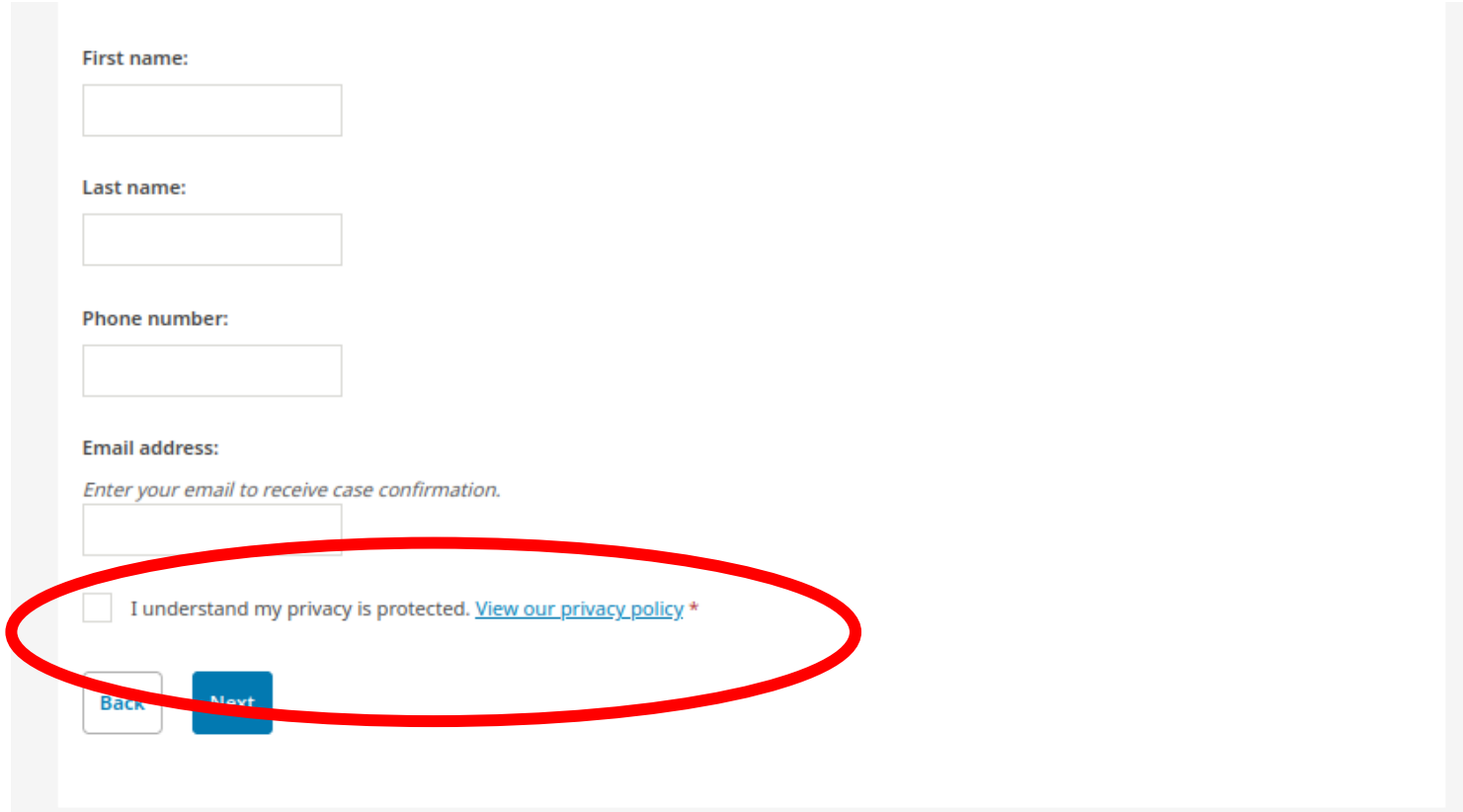
Url	Status	Type	Size
https://www.googletagmanager.com/gtag/js?id=G-2PTP2415JR&cx…	200	script	0 B
https://www.google-analytics.com/analytics.js	200	script	0 B
https://www.google-analytics.com/j/collect?v=1&_v=j102&a=18777…	200	xhr	26 B
https://van311.ca/_media/ws/cov/vanconnect-home-data.json	200	xhr	861 B
https://van311.ca/__data/assets/image/0024/21669/favicon-32x32.…	200	png	0 B
https://van311.ca/_media/pwa/cov-favicons/android-icon-144x144.…	200	png	11.8 kB
https://analytics.google.com/g/collect?v=2&tid=G-2PTP2415JR&gt…	204	fetch	20 B
https://van311.ca/services/pothole	200	document	8.7 kB
https://cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js	200	script	0 B
https://van311.ca/__data/assets/css_file_folder/0025/9853/wss.css	200	stylesheet	0 B

METHODS: PRIVACY POLICIES

What data is collected and why and with whom is it shared?

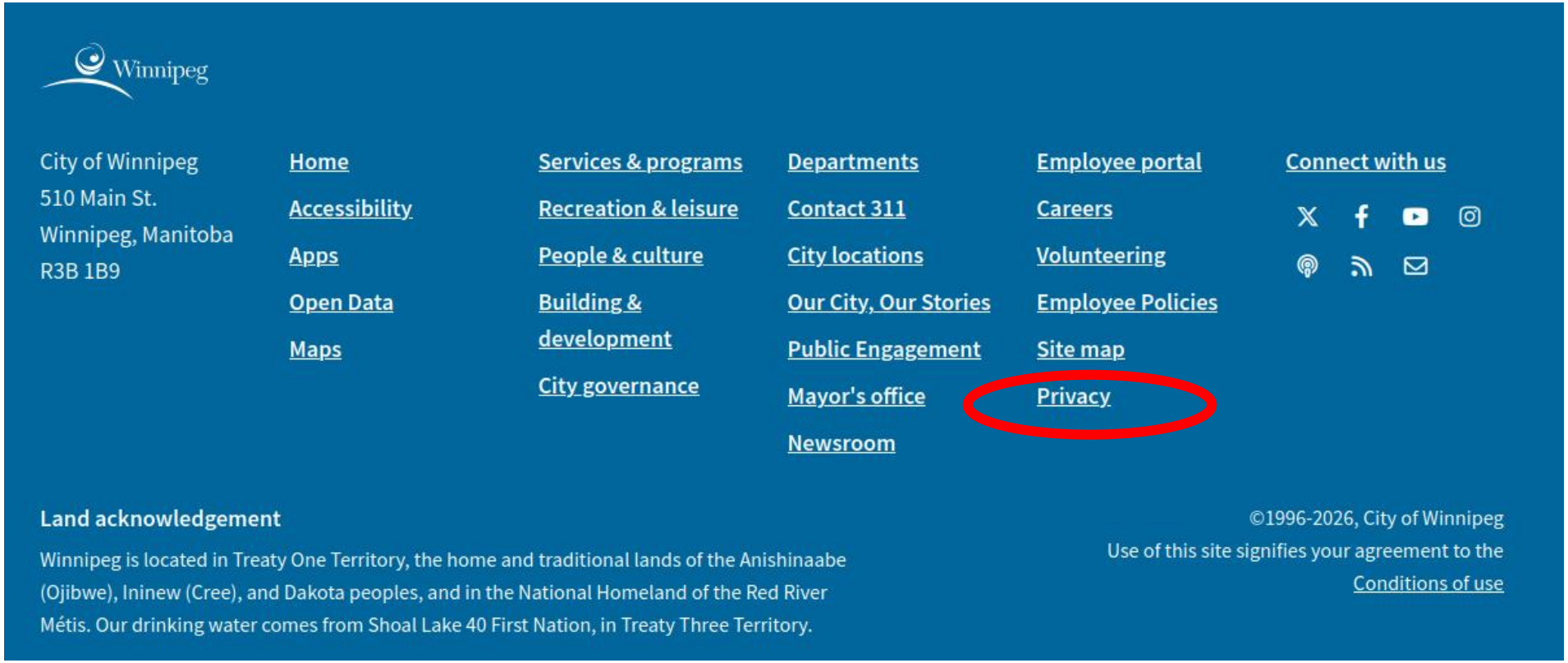
Where is the privacy policy?

- Linked to or referenced within submission interface



Where is the privacy policy?

- Linked to or referenced within submission interface
- Linked to in the footer of the submission interface



Where is the privacy policy?

- Linked to or referenced within submission interface
- Linked to in the footer of the submission interface
- Available through the city's homepage (not the 311 website)



Calgary.ca privacy statement

The City of Calgary is committed to providing a website that respects your privacy. This statement summarizes the privacy policy and practices on the calgary.ca website and all associated systems, processes and applications under the direct control of The City of Calgary. The City of Calgary is subject to Alberta's Access to Information Act (ATIA) and Protection of Privacy Act (POPA).

Where is the privacy policy?

- Linked to or referenced within submission interface
- Linked to in the footer of the submission interface
- Available through the city's homepage (not the 311 website)
- Does not exist

From each policy, we extract:

- Explicit terms used to define personal and device information
- What third parties and their practices are named
- What is mentioned about collection, use, share, retention, and protection of:
  - Personal information
  - Device information
  - Information explicitly provided by visitors through their correspondence or implicitly collected by web servers

KEY RESULTS

Personal Data Collected Through UI

TABLE II: Most amount of required PII collected via the UI across all 6 service request types.

City	First Name	Last Name	Email	Phone	Address	Location	Attachment	Details
Calgary	○	○	○	○	○	●	○	●
Halifax	●	●	●	●	–	●	○	●
Iqaluit	●	●	○	●	○	–	○	○
Moncton	●	●	●	●	–	●	○	●
Montreal	●	●	●	○	–	●	○	●
Ottawa	●	●	●	●	●	●	○	●
Saskatoon	●	●	●	●	◐	●	○	●
St. John's	–	–	–	–	–	●	○	●
Toronto	●	●	●	●	○	●	○	●
Vancouver	●	●	●	●	–	●	○	●
Whitehorse	●	●	●	●	○	◐	○	○
Winnipeg	●	●	○	●	–	●	○	●
Yellowknife	●	●	●	○	–	●	○	○

Legend: ● = required, ○ = optional, ◐= implied, – = not requested.

Personal Data Collected Through UI

Location of the issue (almost always required)

TABLE II: Most amount of required PII collected via the UI a equest types.

City	First Name	Last Name	Email	Phone	Address	Location	Attachment	Details
Calgary	○	○	○	○	○	●	○	●
Halifax	●	●	●	●	–	●	○	●
Iqaluit	●	●	○	●	○	–	○	○
Moncton	●	●	●	●	–	●	○	●
Montreal	●	●	●	○	–	●	○	●
Ottawa	●	●	●	●	●	●	○	●
Saskatoon	●	●	●	●	◐	●	○	●
St. John's	–	–	–	–	–	●	○	●
Toronto	●	●	●	●	○	●	○	●
Vancouver	●	●	●	●	–	●	○	●
Whitehorse	●	●	●	●	○	◐	○	○
Winnipeg	●	●	○	●	–	●	○	●
Yellowknife	●	●	●	○	–	●	○	○

Legend: ● = required, ○ = optional, ◐= implied, – = not requested.

Personal Data Co ugh UI

Name (frequently required)

TABLE II: Most am collected via the UI across all 6 service request types.

City	First Name	Last Name	Email	Phone	Address	Location	Attachment	Details
Calgary	○	○	○	○	○	●	○	●
Halifax	●	●	●	●	–	●	○	●
Iqaluit	●	●	○	●	○	–	○	○
Moncton	●	●	●	●	–	●	○	●
Montreal	●	●	●	○	–	●	○	●
Ottawa	●	●	●	●	●	●	○	●
Saskatoon	●	●	●	●	◐	●	○	●
St. John's	–	–	–	–	–	●	○	●
Toronto	●	●	●	●	○	●	○	●
Vancouver	●	●	●	●	–	●	○	●
Whitehorse	●	●	●	●	○	◐	○	○
Winnipeg	●	●	○	●	–	●	○	●
Yellowknife	●	●	●	○	–	●	○	○

Legend: ● = required, ○ = optional, ◐= implied, – = not requested.

Personal Data Collected Through UI

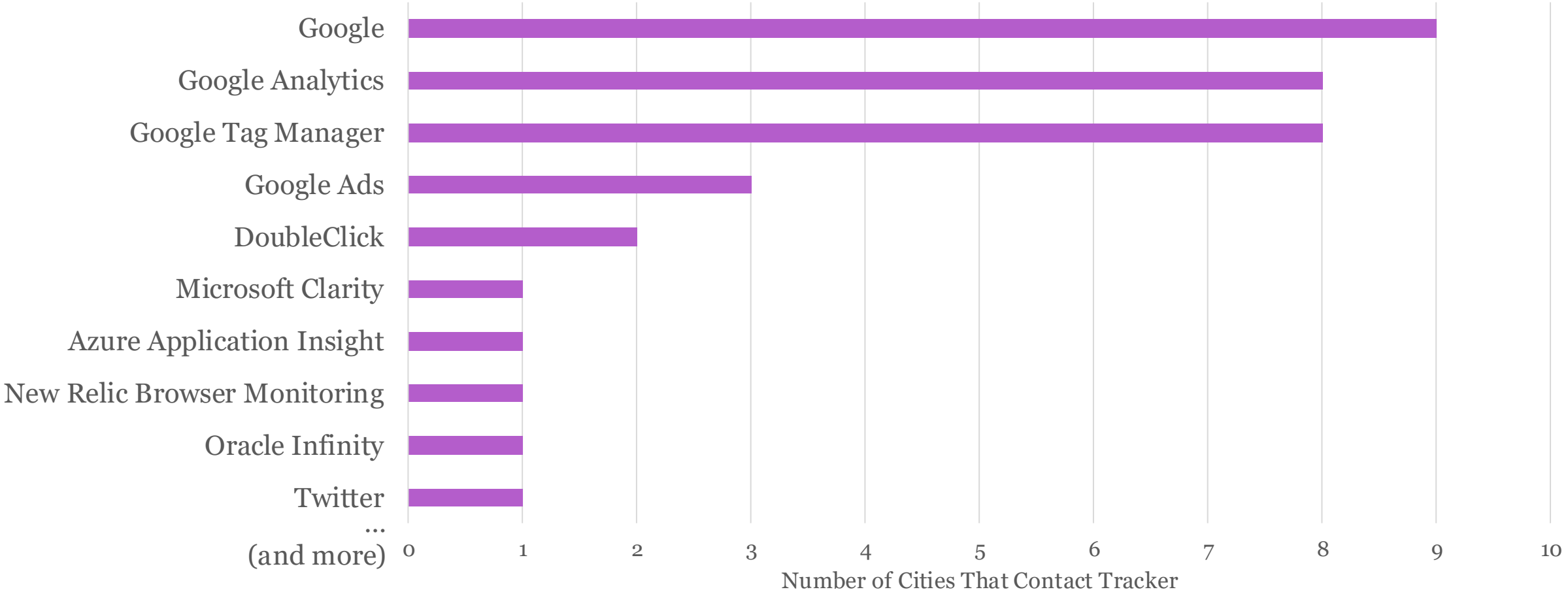
TABLE II: Most amount of required PII collected via the UI across all 6 service request types.

City	First Name	Last Name	Email	Phone	Address	Location	Attachment	Details
Calgary	○	○	○	○	○	●	○	●
Halifax	●	●	●	●	–	●	○	●
Iqaluit	●	●	○	●	○	–	○	○
Moncton	●	●	●	●	–	●	○	●
Montreal	●	●	●	○	–	●	○	●
Ottawa	●	●	●	●	●	●	○	●
Saskatoon	●	●	●	●	◐	●	○	●
St. John's	–	–	–	–	–	●	○	●
Toronto	●	●	●	●	○	●	○	●
Vancouver	●	●	●	●	–	●	○	●
Whitehorse	●	●	●	●	○	◐	○	○
Winnipeg	●	●	○	●	–	●	○	●
Yellowknife	●	●	●	○	–	●	○	○

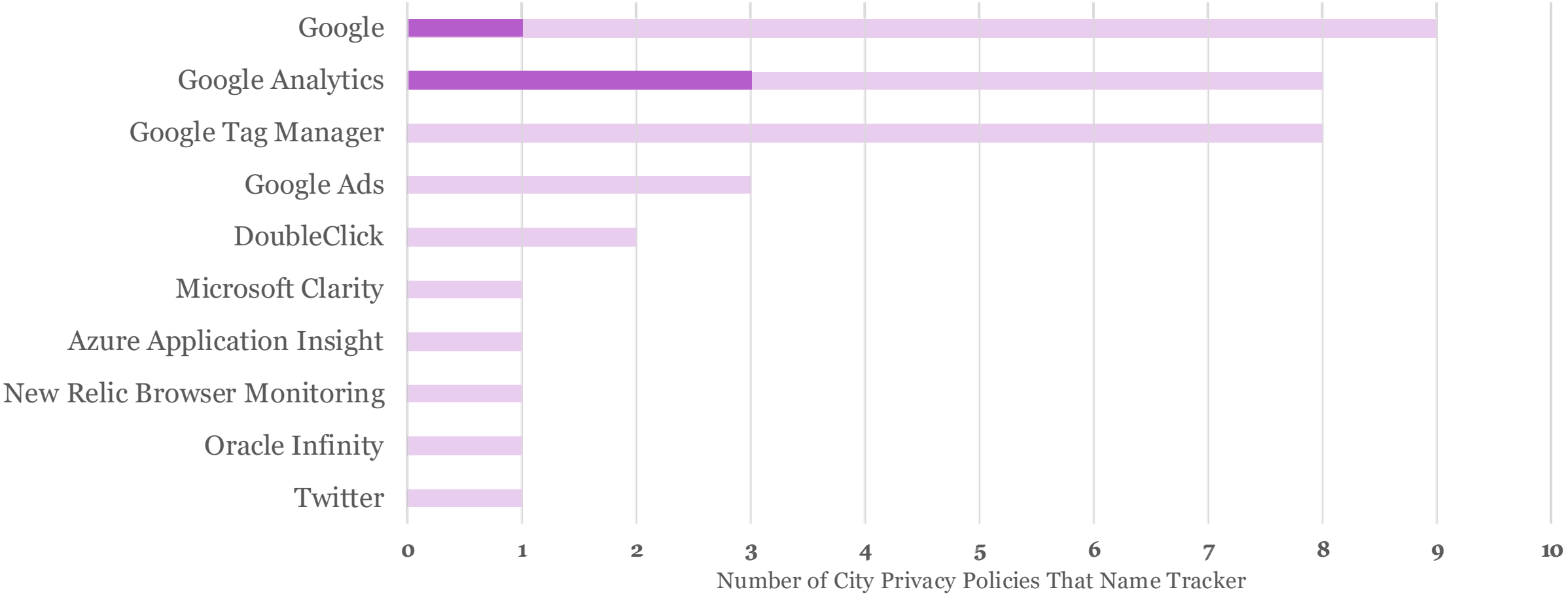
Legend: ● = required, ○ = optional, ◐= implied, – = not requeste

Attachments (always optional)

All Cities Contact Trackers



Contacted Trackers Named in Privacy Policies



Citizens are Left to Understand Third-Party Practices Themselves

The City uses Google Analytics for reports on website traffic and use, Google Analytics collects first-party cookies, data related to the device/browser, IP address, and website activities to measure and report statistics about user interactions on the websites. For more information on what data is collected and used by Google Analytics, see their page on Data Privacy and Security. To opt-out, visit Google Analytics Opt-out.

Citizens are Left to Understand Third-Party Practices Themselves

The City uses Google Analytics for reports on website traffic and use, Google Analytics collects first-party cookies, data related to the device/browser, IP address, and website activities to measure and report statistics about user interactions on the websites. For more information on what data is collected and used by Google Analytics, see their page on Data Privacy and Security. To opt-out, visit Google Analytics Opt-out.

Safeguarding your data

Laws protecting user privacy such as the European Economic Area's General Data Protection Regulation and other privacy laws that establish various rights for applicable US-state residents impact content publishers, application developers, website visitors, and application users. See also the Google privacy policy and Google's site for customers and partners. Currently such regulations apply to specific geographic regions, but publishers and application developers often implement controls that affect the experience of users in all regions.

Google is committed to protecting data confidentiality and security. It is important to understand your privacy options, whether in the role of a publisher or a consumer. This page provides information on data collection and security for:

- Content publishers and app developers ("customers") using Google measurement products.
- Website visitors and app users ("users") of sites and apps using Google measurement products.

Data collection

Google customers use tags on web pages and an SDK for mobile apps to enable Google measurement products. The measurement data collected helps customers understand their users' needs and, optionally, personalize the user experience and offer relevant advertising (see Advertising personalization).

Google tags and the SDK use cookies and app instance IDs, respectively, to measure user interaction. While these identifiers provide information about user behavior, Google prohibits customers from sending Personally Identifiable Information to Google Analytics. Even so, use of cookies and app IDs falls under the privacy laws mentioned previously. Google customers need to inform users about the information being stored and give them the opportunity to grant or deny their consent.

See the following sections on this page to:

- Learn how Google collects and processes information about website and app usage: Information for sites and apps using Google Analytics.
- Learn about our user policies and controls: Information for visitors of sites and apps using Google Analytics.

Download this diagram that explains how Google Analytics collects, filters, and stores data.

Information for visitors of sites and apps Using Google Analytics

Our privacy policy

At Google, we are keenly aware of the trust you place in us and our responsibility to keep your privacy and data secure. As part of this responsibility, we let you know what information we collect when you use our products and services, why we collect it, and how we use it to improve your experience. The Google privacy policy & principles describes how we treat personal information when you use Google's products and services, including Google Analytics.

Google Analytics cookies and identifiers

Google Analytics mainly uses first-party cookies to report on visitor (aka. user) interactions on Google Analytics customers' websites. Users may disable cookies or delete any individual cookie. Learn more about How Google uses cookies

In addition, Google Analytics supports an optional browser add-on that - once installed and enabled - disables measurement by Google Analytics for any site a user visits. Note that this add-on only disables Google Analytics measurement.

Where a site or app uses Google Analytics for Apps or the Google Analytics for Firebase SDKs, Google Analytics collects an app-instance identifier — a randomly generated number that identifies a unique installation of an App. Whenever a user resets their Advertising Identifier (Advertising ID on Android, and ID for Advertisers on iOS), the app-instance identifier is also reset.

Where sites or apps have implemented Google Analytics with other Google Advertising products, like Google Ads, additional advertising identifiers may be collected. Users can opt-out of this feature and manage their settings for this cookie using the Ads Settings. Learn more about Purposes of cookies

Information for sites and apps using Google Analytics

Google Analytics under the General Data Protection Regulation (GDPR)

Google operates as a data processor for Google Analytics. This is reflected in our Ads Data Processing Terms, which are available to all Google Analytics customers with direct contracts with Google. Learn more about Data Processing Terms

Google Analytics is a data processor under GDPR because Google Analytics collects and processes data on behalf of our clients, pursuant to their instructions. Our customers are data controllers who retain full rights over the collection, access, retention, and deletion of their data at any time. Google's use of data is controlled by the terms of its contract with Google Analytics customers and any settings enabled by customers through the user interface of our product.

Google Analytics under privacy laws in the United States

In order to help Google Analytics customers prepare for laws that establish various rights for applicable US-state residents, we have updated our Data Processing Terms to include a *U.S. State Privacy Laws Service Provider and Processor Addendum*. Subject to the full terms of this addendum, Google Analytics will act as a service provider to its customers (when data sharing with Google products and services is disabled) and as such, will only use data collected on behalf of the customer in Google Analytics to provide the Google Analytics services. Customers who have not accepted our Data Processing Terms can do so per these instructions. Customers who have already agreed to our Data Processing Terms will not need to take additional action to accept the CCPA service provider addendum. Customers should review the *U.S. State Privacy Laws Service Provider and Processor Addendum*, as well as Google Analytics' use of data, to ensure it meets customer's compliance needs.

To help customers manage their compliance needs, Google Analytics offers a collection of tools, detailed below, that enable you to control how data is collected, and whether it is used for advertising personalization.

If you have linked Google Analytics to another product, please refer to Google Analytics linking overview.

Google Analytics under the Lei Geral de Proteção de Dados (LGPD)

Google operates as a data processor for Google Analytics. This is reflected in our Ads Data Processing Terms, which are available to all Google Analytics customers with direct contracts with Google. Learn more about Data Processing Terms.

Google Analytics is a data processor under LGPD because Google Analytics collects and processes data on behalf of our clients, pursuant to their instructions. Our customers are data controllers who retain full rights over the collection, access, retention, and deletion of their data at any time. Google's use of data is controlled by the terms of its contract with Google Analytics customers and any settings enabled by customers through the user interface of our product.

International transfers

See here for information on data transfers via Google Analytics.

Data Collected by Google Analytics

First-party cookies

Google Analytics collects first-party cookies, data related to the device/browser, IP address (when collecting data, Google Analytics does not log or store IP addresses), and on-site/app activities to measure and report statistics about user interactions on the websites and/or apps that use Google Analytics. Customers may customize cookies and the data collected with features like cookie settings, User-ID, Data Import, and Measurement Protocol. Learn more about Website data collection

Google Analytics customers who have for instance, enabled the analytics.js or gtag.js collection method can control whether or not they use cookies to store a pseudonymous or random client identifier. If the customer decides to set a cookie, the information stored in the local first-party cookie is reduced to a random identifier (e.g., 12345.67890).

For customers who use the Google Analytics for Apps SDK, we collect an App Instance Identifier, which is a number that is randomly generated when the user installs an app for the first time.

Advertising identifiers

Where customers use Google Analytics Advertising Features, Google advertising cookies are collected and used to enable features like Remarketing on the Google Display Network. These features are subject to the users' Ads Settings, the Policy requirements for Google Analytics Advertising Features and Google's EU User Consent policy, which requires customers to obtain consent for cookies where legally required—including consent for personalized ads. For more information about how Google uses advertising cookies, visit the Google Advertising Privacy FAQ. It is possible to implement Google Analytics without affecting normal data collection where Advertising features are disabled until consent is obtained (see Privacy Controls in Google Analytics), as well as prevent certain data from being used for advertising personalization purposes (See Advertising Personalization below).

PII prohibition

Our contracts prohibit customers from sending Personally Identifiable Information to Google Analytics. Customers should follow these Best Practices to ensure PII is not sent to Google Analytics.

What is the data used for?

Google uses Google Analytics data to provide the Google Analytics measurement service to customers. Identifiers such as cookies and app instance IDs are used to measure user interactions with a customer's sites and/or apps, while IP addresses are used to provide and protect the security of the service, and to give the customer a sense of where in the world their users come from. Customers may also choose to use the data collected by Google Analytics for site/app personalization or advertising purposes, including ads personalization (See Advertising Personalization below).

Data access

We do not share Google Analytics data without the customer's authorization (including via settings in the product user interface), or as otherwise expressly permitted under the terms of their Google Analytics agreement, except in limited circumstances when required by law.

Customers may control their own access to data in their Analytics accounts or properties by configuring view and edit permissions for employees or other representatives who may login to their Analytics account. Learn more about Add, edit, and delete Analytics users and user groups

Security-dedicated engineering teams at Google guard against external threats to data. access to data (e.g., by employees) is limited by strict access controls (both internal poli controls and automated technical controls such as authentication, SSL, and security log those with a business need to access it.

Product linking summary

Where customers link their Analytics property to another Google product or service acc ("Integration Partner"), certain data from that Analytics property may be accessed and into the linked account. Once data is exported through a linking integration, it becomes the Integration Partner's terms and policies.

Note that once data is sent to an Integration Partner, that the data sent is subject to the that Integration Partner and that Google Analytics no longer maintains access or control data.

Customers may review and manage their product integration linkings at any time within t Analytics product linking summary user interface.

Data sharing

Google Analytics provides several data sharing settings to customers, through which cu may customize how data collected using an Analytics data collection method (like the Ja code, mobile SDKs, and the Measurement Protocol) may be accessed and used by Goog according to customer preferences. Note that these settings only apply to data collecte websites, mobile apps, and other digital devices using Analytics; they do not apply to da to a customer's use of Analytics, such as the number of properties and which additional are configured. Regardless of a customer's data sharing settings, Analytics data may als only insofar as necessary to maintain and protect the Analytics service. Learn more abo sharing settings

Data Controls for retention, deletion, and portability

Data retention

With the Data Retention controls, customers can limit or expand the duration for which t level and event-level data is stored in Google Analytics servers. All customers should rev Data Retention settings and ensure the appropriate retention is selected.

User deletion

Customers may delete a single user's data from Google Analytics by passing a single us identifier to the Google Analytics User Deletion API or via our User Explorer report. H this does not delete aggregate data associated with that user, such as page URLs visite

User-level data access and portability

Customers may pull event information for any given user identifier via our User Explorer the User Activity API. These features enable customers to analyze and export event level a single user identifier. In addition, our 360 customers may integrate with BigQuery to cr export of all event data associated with their users in a single queryable repository.

Advertising personalization

Customers may choose to limit use of their analytics data for advertising personalization purposes, instead of disabling the collection of all analytics data or advertising identifier "Privacy Controls in Google Analytics"). Customers may choose to disable Advertising Personalization for data collected from their entire property, or to disable it for individua or users (for apps, websites, and measurement protocol). Customers using Goo Analytics for Firebase or Google Analytics properties may also exclude specific events o properties (like 'purchase' or 'gender') from being used for Ads Personalization.

If any of 1) all property-level data, 2) individual events, or 3) specific event names or use properties have been excluded from ads personalization, then Analytics will append an signal (called 'npa') in Postbacks indicating that networks should not use the data for personalized advertising. Note that each network's treatment of such 'npa' signal is dete such network.

Data privacy and security

Certifications

ISO 27001

Google has earned ISO 27001 certification for the systems, applications, people, techno processes, and data centers serving a number of Google products, including Google An Learn more about ISO 27001 Certification or Learn more about ISO compliance, and dov our certificate (PDF)

Information security

In web-based computing, security of both data and applications is critical. Google dedic significant resources towards securing applications and data handling to prevent unauth access to data.

Data is stored in an encoded format optimized for performance, rather than stored in a t file system or database manner. Data is dispersed across a number of physical and logic volumes for redundancy and expedient access, thereby obfuscating it from tampering.

Google applications run in a multi-tenant, distributed environment. Rather than segregat customer's data onto a single machine or set of machines, data from all Google users (c business, and even Google's own data) is distributed among a shared infrastructure com Google's many homogeneous machines and located in Google's data centers.

In addition, Google Analytics ensures secure transmission of its JavaScript libraries and measurement data. Google Analytics by default uses HTTP Strict Transport Security (HS instructs browsers that support HTTP over SSL (HTTPS) to use that encryption protocol communication between end users, websites, and Google Analytics servers. Learn more How Google Analytics secures your web traffic

Operational security and disaster recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, Google implements a comprehensive disaster-recovery program at all of its data centers. This program includes multiple components to eliminate single points of failure, including the following:

Data replication: To help ensure availability in the event of a disaster, Google Analytics data stored in Google's distributed file system is replicated to separate systems in different data centers.

Geographical distribution of data centers: Google operates a geographically distributed set of data centers that is designed to maintain service continuity in the event of a disaster or other incident in a single region.

Resilient and redundant infrastructure: Google's computing clusters are designed with resiliency and redundancy in mind, helping minimize single points of failure and the impact of common equipment failures and environmental risks.

Continuity plan in the event of disaster: In addition to the redundancy of data and regionally disparate data centers, Google also has a business-continuity plan for its headquarters in Mountain View, CA. This plan accounts for major disasters, such as a seismic event or a public-health crisis, and it assumes people and services may be unavailable for up to 30 days. This plan is designed to enable continued operations of our services for our customers.

Give feedback about this article

Was this helpful?

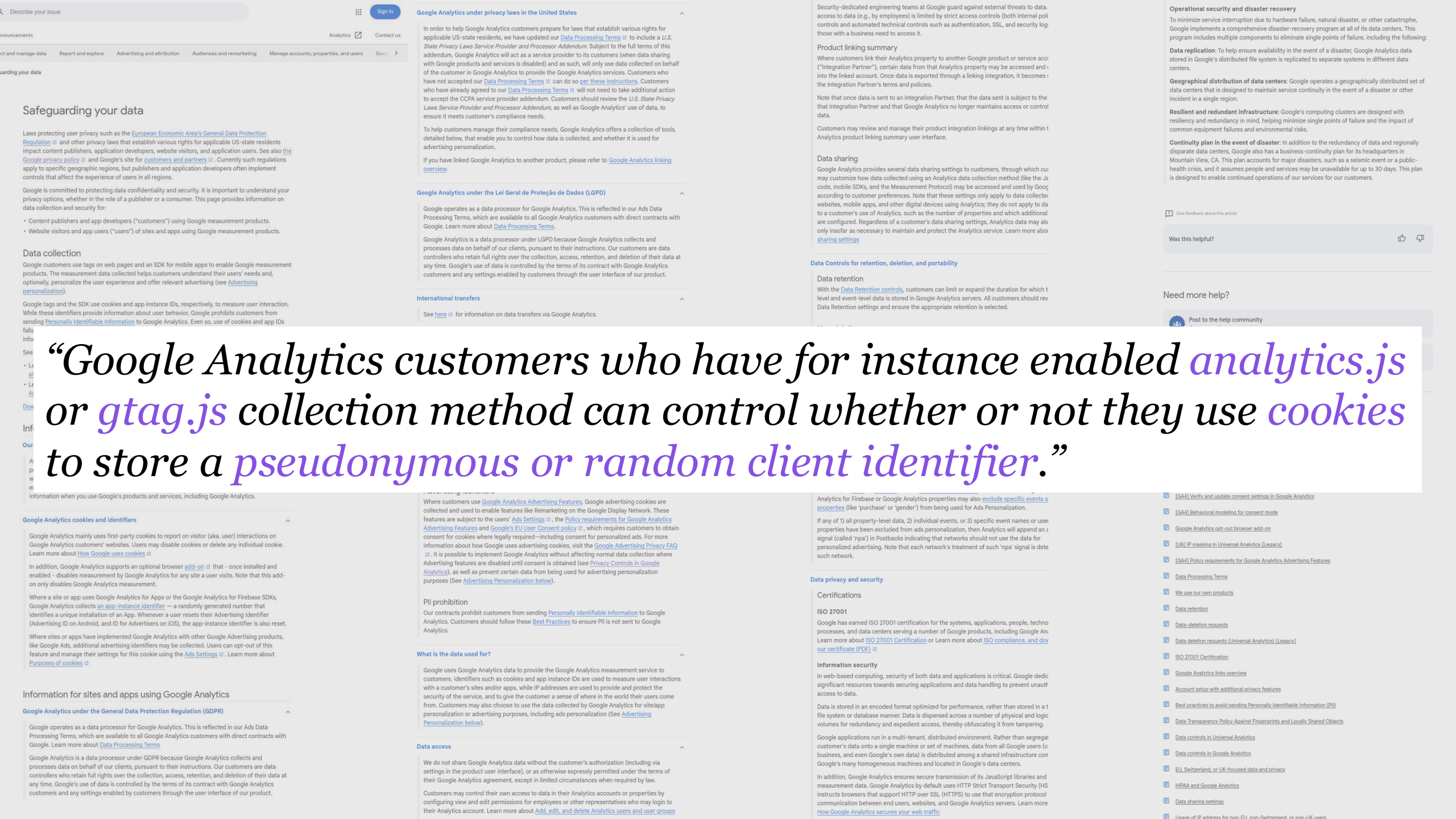
Need more help?

Post to the help community
Get answers from community members

Contact us
Tell us more and we'll help you get there

Data privacy and security

Safeguarding your data
Privacy controls in Google Analytics
[GA4] Data redaction
Introduction to user consent management
[GA4] Verify and update consent settings in Google Analytics
[GA4] Behavioral modeling for consent mode
Google Analytics opt-out browser add-on
[UA] IP masking in Universal Analytics [Legacy]
[GA4] Policy requirements for Google Analytics Advertising Features
Data Processing Terms
We use our own products
Data retention
Data-deletion requests
Data deletion requests (Universal Analytics) [Legacy]
ISO 27001 Certification
Google Analytics links overview
Account setup with additional privacy features
Best practices to avoid sending Personally Identifiable Information (PII)
Data Transparency Policy Against Fingerprints and Locally Shared Objects
Data controls in Universal Analytics
Data controls in Google Analytics
EU, Switzerland, or UK-focused data and privacy
HIPAA and Google Analytics
Data sharing settings
Usage of IP address for non-EU, non-Switzerland, or non-UK users



“Google Analytics customers who have for instance enabled analytics.js or gtag.js collection method can control whether or not they use cookies to store a pseudonymous or random client identifier.”

Other Challenges to Understand Privacy Policies

Other Challenges to Understand Privacy Policies

- All government services/operations are consolidated under one policy.

Other Challenges to Understand Privacy Policies

- All government services/operations are consolidated under one policy.
- It is unclear what information is collected and why.
  - *"We only collect, retain and use personal information where we believe it is essential (and allowed by law) to administer our business and to provide products, services and other opportunities requested by our customers."*

Other Challenges to Understand Privacy Policies

- All government services/operations are consolidated under one policy.
- It is unclear what information is collected and why.
  - *"We only collect, retain and use personal information where we believe it is essential (and allowed by law) to administer our business and to provide products, services and other opportunities requested by our customers."*
- Data management and retention practices are often missing.
  - *"Personal information is only disposed of according to a records retention schedule."*

Other Challenges to Understand Privacy Policies

- All government services/operations are consolidated under one policy.
- It is unclear what information is collected and why.
  - *"We only collect, retain and use personal information where we believe it is essential (and allowed by law) to administer our business and to provide products, services and other opportunities requested by our customers.*
- Data management and retention practices are often missing.
  - *"Personal information is only disposed of according to a records retention schedule."*
- Contain vague language and massive disclaimers.
  - *"The City of St. John's takes reasonable and appropriate measures to safeguard against unauthorized disclosures of personal information. However, the City cannot guarantee that personal information collected will never be accessed, used, lost, or disclosed in a manner that is inconsistent with this Privacy Statement."*

Broader Implications and Next Steps

- A 311 site is meant to build trust, so third-party tracking is a concern.
  - Why are Canadian cities using Google Analytics? “Analytics” can be done locally.

Broader Implications and Next Steps

- A 311 site is meant to build trust, so third-party tracking is a concern.
  - Why are Canadian cities using Google Analytics? “Analytics” can be done locally.
- Developers create websites by combining elements from different sources that are intended for specific uses but may transmit data for other purposes.
  - Understanding purpose remains an open problem.

Broader Implications and Next Steps

- A 311 site is meant to build trust, so third-party tracking is a concern.
  - Why are Canadian cities using Google Analytics? “Analytics” can be done locally.
- Developers create websites by combining elements from different sources that are intended for specific uses but may transmit data for other purposes.
  - Understanding purpose remains an open problem.
- Future work: What are developers seeing / being told through, e.g., documentation?

Broader Implications and Next Steps

- A 311 site is meant to build trust, so third-party tracking is a concern.
  - Why are Canadian cities using Google Analytics? “Analytics” can be done locally.
- Developers create websites by combining elements from different sources that are intended for specific uses but may transmit data for other purposes.
  - Understanding purpose remains an open problem.
- Future work: What are developers seeing / being told through, e.g., documentation?
- Who should take on the custodial role to safeguard consumer data?

There's a (pot)hole in your privacy policy: Privacy Concerns in Canadian Problem-Reporting Websites

Name: Indrani Ray

Email: iray@uwaterloo.ca

LinkedIn: indrani-ray

Summary

- Analyzed how Canadian cities handle personal data when citizens request 311 services online by comparing what is visible through the interface to what is transmitted through the network to what is written in the privacy policy.
- Citizens need to supply personal and personally identifiable information for service requests.
- During these requests, 311 sites are contacting third parties which track visitors.
- However, citizens are not explicitly notified of their data being shared with third parties while submitting these requests.
- Moreover, data handling practices are not properly disclosed in privacy policies (if they exist).

UNIVERSITY OF
WATERLOO



FACULTY OF ENGINEERING