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

Indrani Ray
Electrical and Computer Engineering
University of Waterloo
Waterloo, Canada
indrani.ray@uwaterloo.ca

Maria Wolters
Computer Science
Dortmund University of Applied Sciences and Arts
Dortmund, Germany
maria.wolters@fh-dortmund.de

Kami Vaniea
Electrical and Computer Engineering
University of Waterloo
Waterloo, Canada
kami.vaniea@uwaterloo.ca

***Abstract*—City governments are leveraging digital platforms to increase engagement from the community and make services more accessible to their constituents. These platforms allow citizens to access non-emergency (a.k.a. 311) services to do things like report infrastructure problems, raise environmental concerns, and give feedback to city employees. These digital platforms often require users to supply personal information such as name, phone number, email, and address.**

We examine 13 Canadian cities to understand (i) what information citizens are required to provide across different service requests, (ii) what data is sent to known trackers and other third parties in the network traffic during a pothole repair request, and (iii) what data collection practices and protections are disclosed in privacy policies. We find all cities require citizens to provide personal or personally identifiable information across different services. All cities contact trackers, most-commonly Google services, but only two avoid sending identifiable information to them. Finally, we identify gaps in privacy policies. For example, no city lists all third parties citizen data is sent to.

Although citizens expect transparency and responsible handling of their data from governments, we briefly discuss why this is difficult. The online nature of these systems places responsibility on developers for handling end-user data, but developers themselves might have difficulty understanding or limited visibility into data practices of third parties they integrate with. Our results highlight the need for more transparency around and understanding about third-party data sharing in e-governance.

***Index Terms*—e-governance, online tracking, privacy policies**

I. Introduction

While maintaining infrastructure is the role of municipalities, they often rely on citizens to report problems. For example, the Canadian city of Néal, founded in the 17th century, is responsible for a road network of 4100 km [1]. It is impossible to monitor the entire network, grown historically, without citizens' active cooperation in, for example, reporting problems such as potholes and broken traffic signals. In North America, citizens use a non-emergency service for such problem reports. When the first such services were created in the 1990's, they were bundled under a 311 service hotline (c.f. Table I), modeled on the highly successful 911 emergency phone contact line [2]. With the advent of e-government, online reporting interfaces were integrated into the 311 infrastructure, making reports easier to administer and analyze [2]–[4]. From the point of view of e-government, 311 platforms are a form of e-participation, more specifically e-consultation [5], where citizens provide municipalities with data about local infrastructure.

Privacy and security are key factors in the successful adoption of e-government services [6]–[8]. In their comprehensive recent literature review on the determinants of e-government adoption, Tremblay-Cantin et al. [7] identified two pertinent groups of factors: 1) citizen trust and 2) evaluated risk and security. The first group, *citizen trust*, focuses on citizens' belief that they will not come to harm by using the internet, technology, or e-government services. The second group, *evaluated risk and security*, includes use of personal data, potential for data breaches, and transaction security, among other variables. Jater et al. [8] found that data privacy was the biggest concern of young people across Europe when it came to engaging with e-government systems. Finally, citizens to whom their privacy matters, such as vulnerable groups [9] and ethnic minorities [10], are known to avoid using services that they perceive as being privacy-risky.

In the case of online 311 systems, the system should not only be secure, it should also protect citizens' personal data and ensure confidentiality. If a 311 system allows others to directly or indirectly identify potential posters, they can use this information to track where people potentially live and work, especially for those who use the 311 system frequently. This information can be used for purposes ranging from targeted marketing to in-depth profiling for insurance purposes or even stalking, because posters are highly likely to have visited the places for which they report issues. While visiting a 311 site by itself may not seem like a privacy-important activity, today's information economy functions by collecting and collating large amounts of seemingly benign data into profiles. These profiles are then sold to a range of groups including the Immigration and Customs Enforcement (ICE) [11].

Ideally, privacy policies would set out clearly how posters' information is used and protected. However, privacy policies are generally known to be difficult to find on web sites, use technical terms, require a high reading level, cover many dissimilar services, and deflect accountability regarding the

policies and practices of third parties [12], [13]. In Canada, unlike in the EU, government web sites are not required by law to have a privacy policy. Instead, local government privacy regulations may be delegated at least in part to the Province or Territory, and it is possible that there is no designated data protection officer.

To date, little is known about how online 311 platforms in Canada address the areas of security, personal data protection, and confidentiality. In this study, we documented relevant personal data collection and tracking practices of the online 311 platforms of major Canadian municipalities and analyzed the content of relevant privacy policies. Data were collected in 2026 and compared to our prior workshop paper from 2025 where we extensively piloted the methodology [14]. When looking at network data we focused on pothole reporting, a serious issue impacting all parts of Canada that should require minimal personal information to report. Specifically, we investigated:

RQ1 What privacy-related personal data is a user explicitly asked to provide and which of these data are required?

RQ2 Which third-party websites are being contacted when a citizen reports a pothole?

RQ3 Are unique identifiers or large amounts of data being sent to known tracking or advertising companies, such as Google, during a pothole request without user awareness or consent?

RQ4 What third parties are explicitly mentioned in the privacy policy and in what context?

RQ5 What 311-related information (RQ1 and RQ2 outcomes) does the privacy policy state is collected and what statements are made about its use, purpose, and protection?

In 2026, we expanded our data collection to reflect different browsing scenarios (c.f. Section III-D), introduced a taxonomy to differentiate third parties (c.f. Section IV-C), extended network traffic analysis to include post data (c.f. Section IV-C), and included a more in-depth analysis of privacy policies (c.f. Section IV-E).

We explicitly focus on tracking because this affects both citizen trust and evaluated risk. Citizens might be afraid of being harmed as the result of tracking, for example when the tracking data is later collated and sold to malevolent entities. Therefore, a 311 system that extensively uses tracking without alerting citizens breaks valuable trust. Citizens who do not wish to be tracked might evaluate the risk of using a 311 platform to be not worth the benefit.

By comparing what is said in the policy (if anything) and what is done in practice, and by documenting what changed during the time frame of just one year, we outline potential case studies for further investigation.

II. Related Work

A. Personal Data in 311 Platforms

Platforms for reporting infrastructure problems in a municipality come in many different forms. Some platforms, such as the UK's FixMyStreet [15], cover an entire country and forward the reports they receive to municipalities for further processing. Most other platforms, however, are city-specific. Problem reporting platforms vary in almost every aspect possible—whether they are a website or an app, what details need to be provided, what issues can be reported, what, if any, feedback is given, and whether the problem reports are shared as open data. For example, Boston's comprehensive 311 system [4] yields open data that has been repurposed as a pot hole tracker. Data from 311 requests is also used by governments to provide evidence of governments doing something about visible issues [3], [16]

Many problem reporting platforms ask citizens for a form of contact, typically an email address, so that citizens can be notified about the progress of the issue they raised, or they may ask citizens to log in before reporting issues. Most platforms also allow users to attach photos, which is a popular feature [3]. Photo metadata is not necessarily stripped and can contain details such as geographic location and even author. All of these features are sources of personal identifying information.

In addition to contact data, we also chose to treat the locations of the reports themselves as potentially identifying information. People tend to report issues for the communities where they spend substantial amounts of time [17], [18]. Therefore, attackers can easily profile citizens if they can match their contact information with the reports they submitted.

B. Online Tracking

Online tracking has long been recognized as a privacy concern. In 2000, the U.S. Federal Trade Commission released a report [19] explaining the state of online tracking and privacy concerns associated with it. The focus of the report is advertisers creating profiles based on users' actions on web pages and linking or merging these profiles with personally identifiable information (PII). This invisible process, happening without user knowledge, raises concerns. The concerns listed, which are still relevant today, include: online surveillance, re-identification from data that has been purchased or hacked, and unfair practices such as price discrimination. According to the report, privacy policies should disclose services provided by advertisers, but this does not happen.

Although the report was published years ago, we continue to see a theme in tracking research: private information is leaked to third parties without being disclosed to users. This has been studied in the context of online social networks [20], [21]. The authors conclude, respectively, that it is possible for third parties to link personally identifiable information via these social networks and that even non-social-network sites visibly leak private information to prominent aggregators. The authors of the latter work argue that first-party sites should take a "custodial role" to safeguard consumer privacy by preventing leakage and disclose aggregators' abilities to obtain data. But in section VI, we argue this custodianship is difficult for developers especially considering "the Web has evolved to become a Software as a Service mash-up, where site-owners tend to outsource certain functionalities to 3rd parties" [22].

The gap between privacy policy and practice has been studied in different contexts. Libert [23] conducts a study where he automatically compares third parties mentioned in websites' privacy policies to third parties contacted to determine whether users are informed about companies collecting their data, and further assesses the readability of privacy policies of prominent third parties. Other researchers analyze mobile apps to determine whether their privacy policies disclose privacy-sensitive data flows or leakage [24], [25]. Brookman et al. [26] simulate users browsing sites on different devices to detect what information is shared with third parties and can be used to identify users across devices. They analyze the privacy policies and find most allow third parties to collect and use data such as IP addresses and unique cookie identifiers but only a few discuss "enabling third parties to engage in cross-device tracking."

A work that is similar to ours context-wise is that of Starov et al. [27]. They study PII leakage that occurs through website contact forms. They create a web crawler which automatically locates contact forms on websites, populates them with test data, and submits them. They analyze query string, cookie, header, post, and multipart data to determine potential PII leakage. They point out that PII leakage may occur because of "dynamic scripts that will ex-filtrate user information as soon as that is typed into a contact form" which is a concern we share in our experiments where we populate forms without submitting them.

To date, the main descriptive work on analytics used in Government websites that we are aware of was conducted by the team of Heino, Puhtila, and Rauti in Finland, covering Finland and Sri Lanka [28]–[30] Heino et al. [28] assess Finnish public sector websites. They inspect, using Google Chrome's Developer Tools, "headers, payloads, initiator domains and sizes" for "clearly detectable" data sent to analytics services. They also scan privacy policies for mentions of personal data being sent to third parties and analytics being used. They find extensive use of analytics services that collect device information such as IP addresses which are not mentioned in privacy policies. They argue that the number of analytics services used by public sector sites is not justifiable and that privacy policies claim data is processed in a way inconsistent with how it actually is.

C. The Research Gap

Municipal problem reporting done well is an integral component of smart cities. Such systems leverage the power of citizen sensors where digital sensors need to be calibrated with observed data, have not yet been deployed, or are not feasible. Therefore, it is important to prevent harm by unaddressed privacy leaks. While the interplay between privacy and digital participation has received substantial attention [31]–[33], little is known about the PII that are collected in practice, and the tracking practices of 311 services that might negatively impact citizens' privacy.

In this study, we focus on documenting existing tracking practices and uses of PII in major Canadian 311 platforms. We contribute a methodology that can be replicated for other countries, including the EU, and provide an overview of data practices that can be further investigated with citizens that use 311 services. We take a broad approach, jointly analyzing what information a user is directed to supply, with whom information is shared, and what practices are disclosed to them. Network analysis is based on finding identifiers or leakage of large amounts of data. Since we are interested in both use of PII and tracking, we analyse privacy policies further not just for mentions of analytics and data sharing but also for other practices including data use, protection, and retention.

III. Method

This paper is based on two data collections: one in February 2025, documented in a workshop paper [14], and the other in March 2026. In 2026, the data collection was repeated, expanded, and substantially restructured. We describe the data collection process below and note any changes.

For each city, we collected data about personal data requested from users (Section III-C), network traffic (Section III-D), and privacy policy content (Section III-E).

A. Experimental Setup

We conducted our experiments on an Ubuntu 24.04.2 LTS laptop running the official 64-bit build, version 146.0.3856.97, Microsoft Edge. The laptop was physically located in *blinded city*, Canada and with a Canada-associated IP address. In 2025, we conducted our experiments using Google Chrome as it was the most-frequently used browser [34]. Unfortunately, in 2026, several 311 websites were unable to load due to an incompatibility between Chrome and ESRI's geospatial mapping software [1] used by these sites. We considered several Chromium alternatives and selected Edge due its popularity and features to disable anti-tracking measures, thereby creating a permissive, worst-case configuration, instead of other browsers such as Firefox which set protection measures by default. We further disabled tracking prevention, default extensions, and Copilot Mode.

B. City Selection

We selected the largest city or municipality in each province that had a 311 reporting website. This resulted in 13 cities representing all provinces except Prince Edward Island which had no city or municipality with an online 311 platform. Large cities were chosen because they tend to be early adopters of digital governance services [35] and are more likely to have developed reporting processes.

C. Personal Data Requested

To determine what personal data was requested (**RQ1**), we went through the reporting process for a set of services on each website, stopping at that the final step to avoid submitting fake requests. Cities provide many non-emergency services. Some websites contain a singular form where citizens can

[1] https://www.esri.com/en-us/home

Term	Example Service Request Names
Pothole	Pothole(s), Pothole on the Roadway, Pothole Repair, Report a Pothole, Report a Pothole or Sinkhole, Road Damage, Road Maintenance, Road Pothole
Snow Removal	Roadway Plowing or Sanding Required, Report a Snow Removal Issue, Snow and Ice, Snow and Ice Removal from City Property, Snow Clearing, Snow on City Road, Snow Removal
Tree Maintenance	General Tree Maintenance, Inspect a City Tree, Report Tree Concern, Tree Maintenance, Tree Maintenance Service Requests, Trees, Trees and Plants
Traffic Signal Maintenance	Report a Traffic Signal Malfunction, Report an Issue with a Traffic Light, Traffic/Pedestrian Signal Repair Request, Traffic Signal Inquiry, Traffic Signal Maintenance, Traffic Signal Repair, Traffic Signals
Graffiti Removal	Graffiti Clean Up, Graffiti on City Property Request, Graffiti on Private Property, Graffiti Removal, Report Graffiti
Illegal Parking	Illegal On-Street Parking, Illegally Parked Vehicle, Parking Enforcement, Parking Issues, Parking Violations, Report a Parking Violation, Report a Vehicle in a No Parking Zone

TABLE I: Service request types included in data collection and analysis.

choose from a small set of general services such as "Road Damage" while other sites have multi-page processes where citizens navigate through options resulting in a specific service like "Spongy Moth Infection". We focused on infrastructure-related issues common across cities: potholes, snow removal, tree maintenance, traffic signal maintenance, and graffiti removal. We added illegal parking to include a service that might involve private details of someone other than the person reporting. Table I contains a list of categories and example request names we group under them.

We recorded what types of personal data the website asked for and whether it was required or not. This included personal information such as name and contact information (phone, email, and address) as well as potential personally identifiable information such as location, details, and attachments. The location of the request is likely to be near places the user normally travels, so we included it. Details correspond to free-text components of the submission form where users are encouraged to add additional information about the request which could include identifying information. Attachments are photos or files users can upload which could contain identifying metadata. We labeled each piece of information as 'required' if it was specified as so on the user interface or if its omission lead to an error, 'optional' if it was listed on the form (through, e.g., drop-down menus or short text boxes) but not classified as 'required', and 'implied' if it was not explicitly listed but suggested through additional text on the page (for example, a text box for additional details with a prompt suggesting types of information to include. A user may ignore the prompt or omit such information.).

D. Network Traffic: Third Parties Contacted During Pothole Request

To understand potential privacy loss in regards to third party web connections (**RQ2**, **RQ3**), we recorded HTTP Archive (HAR) files while reporting a pothole starting from the first page of the pothole reporting form until the last step before submission while only providing required information. While analyzing information requested from users across services, we observed that most service-request paths stayed on the same system and requested similar types of personal information. So we anticipated similar network traffic among different requests, and selected potholes to be representative. Furthermore, all Canadian cities experience pothole damage and have support for reporting them.

We follow the methodology presented above, adopted from our prior work [14], but extend it in a few ways. In 2025, a fresh Chrome browser profile was instantiated before each site access. We repeat this process but use Edge instead (see Section III-A). However, this method is limited because there is no browser history. In reality, browsers accumulate identifiers, such as cookies, over time which help third parties track users. So we introduced four browsing scenarios, each beginning with a fresh Edge profile:

Regular - the above methodology.

Signed-in - log into Google account, erase all web activity associated with the account, then proceed to *regular* experiment without further browsing.

Browsing - visit homedepot.ca, usatoday.com, and expedia.ca (details in Appendix A) then proceed to *regular* experiment.

Both - log into Google account, erase all web activity associated with the account, then proceed to *browsing* experiment.

In 2025, we found several 311 websites contacted and sent data to Google-related services, so we included a signed-in condition to examine whether being logged into a Google account affects the information shared. Together, these scenarios represent different combinations of authentication and prior browsing activity that a typical user may encounter.

We extracted four pieces of data from each connection in the HAR files: domain contacted, query strings, cookies, and post data.

We analyzed cookies and GET string values by first looking at them for obvious human-readable terms that might be privacy problematic– we did not find any of these. We then analyzed them for ID-like values. These are random-looking alphanumeric strings that represent globally unique identifiers used by third parties to track users across websites. We used the `zxcvbn` password strength algorithm [36] to find ID-like values. This has been shown to be effective in prior work [37], [38]. In line with prior work, we used a threshold of at least 3 to determine if a value has a high-enough entropy to be a unique ID.

We categorized cookies by their sources and lifetimes. Cookies are either set by Javascript code running on the webpage or in an HTTP response containing a Set-Cookie header [39], so we made a distinction in our analysis by labeling them "Cookie" and "Set-Cookie". We included set-cookies in our network analysis because they can be transmitted in future requests [40]. We made an additional distinction based on lifetimes and categorized cookies as "session" or "persistent". Although both can be used for tracking, session cookies are meant to be used temporarily and are generally deleted once a browser is closed [41]. To make this distinction,

we defined session cookies as those that either did not have an expiration date or had an expiration within a 30-day window from the date of collection.

Finally, we analyzed post data which is often sent to servers when a user uploads a file or enters content into forms on a webpage [42]. There are different types of post data (plaintext, structured JSON, and other MIME types such as multipart form data and images) which make for difficult analysis. Some analyze post data for elements that match cookie, request URI, or device information [21], [22], [43]. We first calculated post data length then manually reviewed the content when large amounts were transmitted to third parties.

E. Privacy Policy Content

For each 311 website we attempted to record a PDF of the privacy policy. If possible, we used the privacy policy linked off the 311 website itself (eight policies found). If not found, we visited the city's homepage, and searched for the city privacy policy instead. The cities of Calgary, Montreal, and Yellowknife had privacy policies that were not accessible directly from the pothole reporting page. The cities of Iqaluit and Whitehorse were missing privacy policies entirely.

We manually inspected each privacy policy and extracted what was mentioned about the collection, use, share, retention, and other protection of personal information, device information, and information either explicitly provided by visitors through their correspondence or implicitly collected by web servers (**RQ5**). To better understand what is protected by these privacy policies, we noted what explicit terms they used to define personal (and device) information. We additionally recorded what third parties and their practices were mentioned in these policies (**RQ4**).

IV. Results

A. Personal Data Requested (*RQ1*)

All but three cities required contact details in some services (Table II). Most cities also required location of the service issue and encouraged citizens to provide further details regarding their service requests.

Cities generally required the same information from citizens for service requests in 2025 and 2026, with some exceptions. Halifax introduced stricter requirements for citizens to provide their name, email, and phone number. Toronto and Whitehorse added additional fields in their forms (Toronto requires details and Whitehorse suggests providing location and, optionally address). In contrast, Saskatoon removed location and attachments from its submission forms (both were previously optional).

B. Third-party Connections (*RQ2*)

We recorded network traffic during pothole requests, and found that all cities contacted third parties in both years. In 2026, cities contacted the same third parties across all browsing scenarios with the exceptions of Vancouver (which contacted `fonts.googleapis.com` under only the `signin` scenario) and Toronto (which contacted `translate-pa.googleapis.com` except under the `signin` scenario). Among the ten most-frequently contacted third parties, seven are Google services. The remaining three are ArcGIS a mapping service, jsDelivr a free Content Delivery Network, and CloudFlare which is also a Content Delivery Network and DDOS Migration company. All cities except Yellowknife contacted a Google service.

C. Data Sent to Trackers (*RQ3*)

We classify contacted sites into three categories. Those with the same domain as the pothole request are *first party* and the rest are *third party*. A subset of third parties are also marked as *trackers* based on DuckDuckGo's Tracker Radar [44] list of prevalent tracking domains. For example, the website to report a pothole in the city of St. John's is `access.stjohns.ca`, and three domains contacted during that process are `maps.stjohns.ca` (first), `stjohns.ic15.esolg.ca` (third), and `www.google.com` (tracker). According to this classification, all cities contacted known trackers (c.f. Table VII). However, St. John's and Yellowknife did not send ID-like information to trackers, and the cities of Calgary, St. John's, Winnipeg, and Yellowknife did not send post data to trackers.

Across all 2026 scenarios, we found a total of 2,362 unique ID-like query string values. 67% of these were sent to trackers and 18.88% were sent to other third parties. The distribution of these values is approximately uniform across browsing scenarios (Table IV). We additionally found 58.34% of ID-like query string values being used for Google services most notably Google Analytics followed by Google Ads and Google Tag Manager.

We eliminated session cookies from our analysis (c.f. section III-D), and were left with 554 ID-like (persistent) cookies. 40.25% of these were sent to trackers but none were sent to other third parties. Table IV shows the distribution of these across browsing scenarios. We saw a greater volume of ID-like cookies transmitted after a Google log-in. Surprisingly, we found fewer cookies in the *browsing* scenario than *regular*. We found 697 ID-like (persistent) set-cookies. 12.62% of these were set by trackers and 62.21% were set by other third parties. Table IV shows the distribution of ID-like persistent set cookies across browsing scenarios. We saw a greater volume of ID-like cookies being set by trackers after a Google log-in.

While the analysis above focuses on connections made to third parties, first-party requests can also raise privacy concerns. This is especially true given the prevalence of Google-owned services engaging in tracking. In particular, Google Analytics sets first-party cookies which track user activity and enable cross-site identification. Table V shows whether cities send ID-like information to Google services.

Website connections can also send data via POST. This method is normally used to send more complex data which can be harder to interpret. Here we focused on the amount of data sent, instead of its content which we will further study in future work. Table VI shows the sum of post data (in bytes) cities sent to various domains. The table includes all observed post data, so the absence of a city-domain entry indicates no post data was sent. During the pothole-reporting process, we only

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.

TABLE III: Required PII collected during pothole request. Two icons: 2025 icon → 2026 icon

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, → = change from 2025 to 2026.

Type of Data	**# Unique ID-like Values**	**% Regular**	**% Signed-in**	**% Browsing**	**% Both**
Third-party					
query string values	310	24.66%	25.11%	24.89%	25.34%
cookies (persistent)	0	0%	0%	0%	0%
set-cookies (persistent)	428	19.86%	32.01%	27.1%	21.03%
Tracker					
query string values	1720	25.38%	24.62%	24.87%	25.13%
cookies (persistent)	223	8.52%	41.7%	7.62%	42.15%
set-cookies (persistent)	88	17.05%	37.5%	11.36%	34.09%

TABLE IV: Distribution of unique ID-like values across different browsing scenarios. "Cookies" are cookies sent from the browser to the server. "Set-cookies" are cookie set requests sent from the server to the client.

provided required input which were text-based entries, so the differences in payload volume are not caused by, for example, uploaded files. Among the non-Google domains being sent considerable amounts of post data are: New Relic which offers browser monitoring services [45], [46], Microsoft Defender an "enterprise endpoint security platform" [47], Microsoft Clarity a behavioral analysis tool [48], and Azure Monitor which enables application performance monitoring [49], [50]. Although not explicitly used for tracking, some requests to Microsoft Defender still contained user information such as language and timezone as well as device information such as browser type and version, screen resolution, and operating system and made calls to Google Analytics with identifiers.

*D. Third Parties Mentioned in Privacy Policies (**RQ4**)*

As mentioned in Section III-E, eight cities had links to their city-wide privacy policies from their 311 sites and three had links from their homepages. The privacy policies were therefore not specific to 311 services, but were applicable to all city-wide practices. Out of these eleven cities, only five explicitly named third parties in their privacy policies. Halifax named Google, Browse Aloud, and AddThis, and also mentioned they collect device information. Montreal referenced Google reCAPTCHA to verify human interactions and named Google Cloud as the "Data Processor" for the service. Montreal also mentioned using Google Analytics to collect statistical information, and that data collected can be transmitted to

City	1st-Party Cookie	3rd-Party Cookie	Query String Value	Google Service Listed in Privacy Policy
Calgary			✓	
Halifax	✓	✓	✓	Google
Iqaluit	✓	✓	✓	N/A
Moncton	✓		✓	
Montreal	✓*	✓	✓	Google Cloud, Google reCAPTCHA, Google Analytics
Ottawa	✓		✓	Google Analytics
Saskatoon	✓	✓*	✓	
St. John's				
Toronto	✓	✓	✓	
Vancouver	✓	✓*	✓	
Whitehorse	✓	✓	✓	N/A
Winnipeg	✓	✓*	✓	Google Programmable Search Engine, Google reCAPTCHA, Google Analytics
Yellowknife				

Legend: ✓= ID-like value sent, ✓* = ID-like value sent when logged-in.

TABLE V: Which cities are sending ID-like values in cookie or query string data to Google-owned services and what Google services are named verbatim in the respective privacy policies.

Google servers outside of Canada. Ottawa named Google Analytics to collect data for statistical purposes, but informed visitors "Google currently offers a free Google Analytics opt-out tool" which was linked to in the privacy policy. Vancouver listed Expo which provides push notifications for their mobile 311 app. Finally, Winnipeg mentioned Google Programmable Search Engine which helps their visitors look for information, Google reCAPTCHA to verify users are human, and Google Analytics to report on web traffic and use. The third parties listed in the privacy policies do not represent the number of third parties contacted during service requests which ranged from 6 to 18. Furthermore, as listed above, the privacy policies often only include company names such as "Google" instead of listing specific services or subsidiaries like "YouTube" (c.f. Table V).

Furthermore, cities were not clear about whom they shared personal or device information with. Calgary was the only city which explicitly claimed it does not share personal or device information to third parties. On the other hand, Montreal mentioned that third parties collect personal information and device information. Four additional cities mentioned that third parties collect device information. Seven cities claimed to not sell, rent, share, exchange, or disclose personal information unless required by law while five mentioned that only authorized personnel (e.g. city staff) can access personal information.

*E. Collection, Use, Retention, and Protection of Information (**RQ5**)*

1) Collection and use: Cities specified two types of information in their privacy policies: personal information and device information. These terms were not explicitly defined, but cities provided examples of what they considered personal or device information. Table VIII lists information explicitly mentioned in privacy policies. Name and email are the most common forms of personal information listed with IP-address and cookies also frequently referenced.

Three cities claimed to automatically collect personal information of visitors to their sites. Three others claimed to collect personal information only when it is voluntarily provided (through, for example, form submission or email correspondence). Calgary, out of these three, further claimed not to collect without notice. Two cities (claimed they do not automatically collect personal information. However, six cities claimed their web servers collect device information with two of these further tracking visitors' browsing habits (such as page navigation). Four cities mentioned third parties collect device information such as browser versions and IP addresses, but these third parties were not always explicitly named as we saw in section IV-D.

Cities were vague about the purpose for which they collect personal information. Seven claimed to collect it to respond to requests and provide services for citizens. Some (23%) said they collect personal information for the purpose it was supplied for. Two cities claimed to use personal information to improve city services. The city of Montreal was the only city which claimed to collect personal information so citizens do not need to re-identify themselves. Saskatoon's privacy policy explicitly stated that personal information is not collected for website operation.

On the other hand, many cities (46%) claimed to collect device information for website operation. Seven cities claimed device information is collected for statistical or analytical purposes. Halifax collected device information to facilitate the security of its online services. Five cities collected this information to enhance visitor experiences on their websites.

In section IV-C we saw many cities sending cookies to trackers to identify users. Toronto's privacy policy echoed this by mentioning the use of persistent cookies to log user activity over multiple visits "with the intent of remembering data, settings, or preferences unique to that visitor." Likewise, Moncton and Montreal's privacy policies mentioned using cookies for retargeting and advertisements. On the other hand, Calgary explicitly stated the information their website collects is not used to identify users.

2) Retention and protection: Cities did not clearly express their retention and data maintenance practices in their privacy policies. Most commonly they referred to city-wide auditing requirements, records retention schedule, or other bylaws though these were not always explicitly named or linked to but referred to by those keywords. The exceptions were Montreal and Vancouver which explicitly named the legislation and Winnipeg which linked to it. Five cities referred to these requirements for the maintenance and disposal of personal information and one city, Calgary, for the maintenance and disposal of device information. Overall, three cities claimed to retain personal information and three claimed to retain device information (Montreal, claimed to do both). None of the cities referred to third party data retention practices.

City	Domain	Regular	Signed-in	Browsing	Both
First-party					
Calgary	calgary-cwiprod.motorolasolutions.com	81	81	81	81
Moncton	moncton.ca	11	11	11	11
Saskatoon	saskatoon.ca	377	377	377	377
Vancouver	van311.ca	3736	3736	3736	3736
Yellowknife	apps.yellowknife.ca	5812	5812	5812	5812
Third-party					
St. John's	stjohns.form.ca.empro.verintcloudservices.com	143	143	143	143
Winnipeg	winnipeg.form.ca.empro.verintcloudservices.com	770	881	770	770
Tracker					
Halifax	google.com	16947	15762	14673	16335
Iqaluit	google.com	23891	19962	17601	17994
Iqaluit	bam.nr-data.net	70244	58662	46900	55326
Moncton	maps.googleapis.com	581	581	580	579
Montreal	google.com	16137	17399	16116	17735
Ottawa	us-mobile.events.data.microsoft.com	1041124	1029323	983881	1028866
Ottawa	google-analytics.com	32	32	32	32
Saskatoon	v.clarity.ms	132030	190543	188860	131384
Saskatoon	canadacentral-1.in.applicationinsights.azure.com	29722	28881	28839	28946
Toronto	google.com	112214	92324	64982	65979
Toronto	translate.googleapis.com	1097	1076	1103	1104
Vancouver	analytics.google.com	689	689	689	689
Whitehorse	google.com	18739	22839	20735	22291

TABLE VI: Total length (bytes) of POST data sent to domain during pothole request across different browsing scenarios.

City	# First-Party Connections	# Third-Party Connections	# Tracker Connections	# Total Connections
Calgary	8	16	8	32
Halifax	8	4	28	40
Iqaluit	4	4	40	48
Moncton	8	4	28	40
Montreal	12	4	24	40
Ottawa	16	12	24	52
Saskatoon	4	4	56	64
St. John's	16	16	16	48
Toronto	8	23	48	79
Vancouver	4	16	33	53
Whitehorse	4	12	56	72
Winnipeg	8	16	44	68
Yellowknife	4	24	4	32

TABLE VII: Distribution of first-party, third-party, and tracker connections by city

Cities tried to encourage visitors that their data is protected. Six cities claimed to take security measures or precautions to protect personal information– the most common measure stated in three cities was "encryption technology". Two cities claimed to adopt "safeguards" against unauthorized disclosure of personal information. Although the cities claimed to implement security measures, four warned that data security cannot be fully guaranteed. Two cities reminded visitors to protect their own devices and passwords. Furthermore, eight cities did not take accountability over the practices of linked sites and two of these cities did not take responsibility for third-party practices. Instead, cities encouraged visitors to understand other parties' privacy policies.

V. Summary of Findings

We looked at municipal problem reporting websites of the largest Canadian city in each province (excluding Prince Edward Island). We focused on data automatically being collected during pothole reporting for consistency. We posed five research questions.

RQ1 We asked what privacy-related personal data a user is explicitly asked to provide and which of these data are required. We learned that most cities ask for: personal information such as name and contact information (email, phone, and address) and potentially personally identifiable information such as location of the request and additional details. Personal information is required depending on the service, but personally identifiable information is almost always required.

RQ2 We asked which third-party websites are contacted when a citizen reports a pothole. We found cities contacted, on average, 11 third parties, many of which were known trackers predominantly Google-related.

RQ3 We asked whether unique identifiers or large amounts of data were being sent to known trackers without user awareness or consent. We found that users were sometimes notified of their data being collected by the city in the submission interface, but were not informed of third-party data collection there and, therefore, unable to consent. We found all but two cities sent unique identifiers to Google services. All but two cities sent post data to third parties, nine of which sent post data to trackers.

RQ4 We asked what third parties are explicitly mentioned in the privacy policy and in what context. We found only six cities named third parties with four of them explicitly listing Google services. Third parties are referenced to collect information for statistical, analytical, and operational purposes to maintain the website.

TABLE VIII: Information explicitly mentioned in privacy policies. Note that many privacy policies use general terms like "personal information" or "behavioral interaction" which are not represented in this table.

	name	email	phone	address	opinions	cookies	device os/make&model/id	browser version&type	screen size	language	geo location	date & time of visit	referrer site	page hits / pages accessed	IP info	HTTPS request logs	files downloaded / names&sizes	pixels
Calgary		✓				✓		✓	✓			✓	✓	✓	✓		✓	
Halifax	✓	✓	✓	✓	✓	✓	✓	✓			✓				✓			
Iqaluit																		
Moncton	✓	✓	✓	✓		✓									✓	✓		✓
Montreal	✓	✓	✓	✓		✓	✓	✓		✓	✓				✓			
Ottawa						✓		✓				✓			✓			
Saskatoon	✓	✓												✓			✓	
St. John's						✓									✓			
Toronto	✓	✓		✓		✓									✓	✓		
Vancouver	✓			✓														
Whitehorse																		
Winnipeg						✓	✓	✓				✓		✓	✓			
Yellowknife							✓	✓				✓	✓	✓	✓			

TABLE IX: Counts of unique third parties: named in privacy policies, contacted during pothole service request process, using ID-like values in cookies or GET strings, and being sent POST data as well as if the privacy policy mentions analytics at all.

City	Third party Mentioned	Third party Contacted	Third party Using ID-like Values	Third party Non-empty POST data	Analytics Mentioned
Calgary	0	6	1	0	✓
Halifax	3	8	6	1	✓
Iqaluit	NA	11	4	2	NA
Moncton	0	8	4	1	✓
Montreal	3	7	3	1	✓
Ottawa	1	9	4	2	✓
Saskatoon	0	15	7	2	✓
St. John's	0	8	1	1	-
Toronto	0	18	8	2	✓
Vancouver	1	13	6	1	-
Whitehorse	NA	17	9	1	NA
Winnipeg	3	15	6	1	✓
Yellowknife	0	7	0	0	✓

RQ5 We asked what 311-related information does the privacy policy state is collected and what statements are made about its use, purpose, and protection. We found cities tended to echo the "minimum necessary" principle [51] to justify collecting personal information and justified collecting device information to help with website operation. Policies did not express data maintenance or retention practices, but some alluded to city-wide standards (such as bylaws and records retention schedules). Privacy policies contained language such as "takes safeguards" and "uses encryption" to assure users their data is protected without providing further details. They also do not take responsibility over third-party practices, and instead encourage visitors to understand third-party privacy policies.

VI. Discussion

A. Trust in Online Government Services

One of the roles of 311 sites is to increase the public's trust in the government's ability to be proactive and deal with issues that the public cares about [3]. Some cities provide pothole maps with the repair status of each one, for example, to demonstrate that the government is being proactive about a key citizen concern. Having a 311 site actively sending data to third party trackers seems to be working against that trust-building goal.

It is easy for people to resign themselves to ubiquitous online tracking which enables surveillance capitalism [52]– even to the persistent use of targeted advertising and discriminatory practices such as online price discrimination. But people may not be as accepting of such technologies on a government website, especially if the resulting data is being sent for use by another government. There is concern of N.S.A.

surveillance especially given that the majority of trackers are U.S.-based [40]. Currently, a Canadian is suing the U.S. Department of Homeland Security because of their subpoena to Google compelling the release of information related to his account [53]. Experts interviewed by the Canadian media on this matter argue that this type of surveillance is unavoidable but encourage citizens to "start thinking about encryption" and "check a box wherever you can that says I want my data in Canada" [54]. Although encryption helps with data confidentiality, we saw in this study that users are not regularly presented with choices about where their data goes.

This is in contrast to the E.U. where legislation focuses on prevention of harm and adopts far more stringent guardrails for tracking. Within this legislative framework, tracking practices on government websites are documented and contested. Based on their analysis of trackers deployed in European Open Government portals, Stepanovic et al. [55] recommended raising public awareness of tracking, removing tracking-based analytics as much as possible, switching to open source web analytics, and conducting regular audits of web analytics solutions. Canadian citizens who would like similar protections need to be far more proactive, engage in data practices that require more digital literacy, and self-organize to raise awareness.

As part of the responsible disclosure process, we contacted the cities prior to publication. We are having ongoing discussions about how cities can improve their services by highlighting the gaps between what information is conveyed to citizens via website interfaces and privacy policies and what is shared with third parties in the background. We hope this conversation helps cities improve transparency around their data practices.

B. Google Tags and Analytics

Google services, including tags and analytics, were the most common types of tracking to be found on Canadian 311 sites. This finding is hardly surprising since these free services are also the most prevalent trackers across the web [39], [56], [57]. Stepanovic et al. [55] also noted the high prevalence of Google Analytics in their sample of European government data services and raised privacy and transparency concerns.

Partially due to Europe's GDPR, Google added controls that developers can use to manage the type of data being sent to Google and how it is used. GDPR notably applies to European Union citizens even if they are not currently physically located in the European Union. As a response, many mobile advertising networks tried to push the burden of complying with these laws onto developers [58].

While working on this paper, we read through getting started guides for Google Analytics and Tag Manager, among others. These guides generally adopt a "developers are responsible" perspective: For example, they instruct developers to be aware of and compliant with regional privacy laws. They encourage developers to set up consent mode if they have end users in the European Economic Area. Consent mode *"receives your users' consent choices from your cookie banner or widget and dynamically adapts the behavior of Analytics, Ads, and third-party tags that create or read cookies"* [59]. But while these tools do exist and are mentioned, they are not necessarily as well supported from a developer usability perspective.

Communicating privacy-related requirements between legal teams and developers is also a known ongoing challenge [60] which can lead to situations where a privacy policy says one thing and the developed code does something else. Such situations may be the cause of our identified discrepancies.

We suspect that while some of the cities we studied included tools like Google Analytics to use its detailed tracking features, others may have installed it for basic features without understanding options to opt-out of data collection. We point out that simple tracking of web visitor numbers and broad locations (IP address geolocation) is quite possible to do without involving Google products, it is just not necessarily as easy or seamless to use.

C. Privacy and the Unknown

Notably most of the city privacy policies we looked at were vague, not specific to the 311 service, and used general language. Such issues are typical for privacy policies which are often ambiguous [61] and challenging to read [12], [62].

Part of the tension is likely caused by the size and complexity of a city. Similar to Google's decision to unify its privacy policies to better enable data sharing between its services [63], cities aim to create a single unified privacy policy. But doing so comes at the cost of specificity as the policy must now cover all city activities. Only a few cities referenced municipal acts under which they collected user data within the submission interface rather than solely linking to a city-wide policy.

Privacy is important in online data safety partially because the future is unknown. In 2020 it was not expected that companies would use data from users for AI training, and now it is a common practice. Governments also change with certain types of data being off-limits from government intrusion under one regime and then used for population profiling under another. Privacy policies try and future proof organizations against changing use of collected data. Similarly, individuals, particularly members of vulnerable groups [9] and ethnic minorities [10], are mindful of the negative consequences of having too much data tracked about them.

VII. Future Work

Purpose is an important part of privacy– users care not only about what data is being accessed but also why it is being accessed and for what purpose. Our analysis of network traffic approximates purpose by using the domain of the contacted website and comparing that domain to a list of known trackers. This approach provides a clear measurement that is easy to replicate, but it also conflates domain with purpose.

Future work should consider the best ways to identify the purpose of such connections to better align them with privacy policy statements. In some cases, the connection purpose is quite clear such as connections to DoubleClick, a tracking

company, being used for tracking. The purpose of other connections are less clear, such as connections to Google-owned services like analytics and maps. Determining the purpose of such Google-related connections is also difficult because of Google's unified privacy policy. In 2012, Google unified the policy to encompass different services [63]. On one hand, this reduces the number of policies users need to read but, on the other, it makes it harder to understand which data will be used and how among different services such as advertising and analytics [64]. Developers may add specific elements to a website for particular purposes– such as a Google mapping component to help users report the location of an issue– but the data transmitted through these elements may be used for purposes beyond what the developer intended.

Accurately identifying how data is used across sites is still an open and challenging problem that requires understanding which sites are contacted, what data is sent, and what is conveyed in the privacy policies of the destination sites. Regulation such as GDPR addresses such issues by ensuring there is a clear data controller. Even then, it is unclear how familiar data controllers are with the privacy policies of all third-party sites contacted. Moreover, such regulation is not universal. In light of these challenges, we hope continued work in this area will help users better understand how their personal data are handled and help hold organizations that collect and share it accountable.

ACKNOWLEDGMENT

Wolters' work was funded by the SPRUNG Programme of the Ministry for Science and Culture of the Federal State of Lower Saxony, Germany, as part of the DIGITOPIAS project (FKZ 11 – 76251- 35/2022 (ZN4003)). Vaniea and Ray acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), funding reference number RGPIN-2024-06737.

REFERENCES

[1] Wikipedia, "Voies de Montréal." [Online]. Available: https://fr.wikipedia.org/wiki/Voies_de_Montr%C3%A9al

[2] A. White and K.-S. Trump, "The Promises and Pitfalls of 311 Data," *Urban Affairs Review*, vol. 54, no. 4, pp. 794–823, Jul. 2018, publisher: SAGE Publications Inc.

[3] S. Hartmann, A. Mainka, and W. G. Stock, "Citizen Relationship Management in Local Governments: The Potential of 311 for Public Service Delivery," in *Beyond Bureaucracy: Towards Sustainable Governance Informatisation*, A. A. Paulin, L. G. Anthopoulos, and C. G. Reddick, Eds. Cham: Springer International Publishing, 2017, pp. 337–353.

[4] D. T. O'Brien, "Using small data to interpret big data: 311 reports as individual contributions to informal social control in urban neighborhoods," *Social Science Research*, vol. 59, pp. 83–96, Sep. 2016.

[5] United Nations, "E-Participation Index." [Online]. Available: https://publicadministration.un.org/egovkb/en-us/About/Overview/E-Participation-Index

[6] E. Panopoulou, E. Tambouris, and K. Tarabanis, "Success factors in designing eParticipation initiatives," *Information and Organization*, vol. 24, no. 4, pp. 195 – 213, 2014.

[7] C.-A. Tremblay-Cantin, S. Mellouli, M. Cheikh-Ammar, and H. Khechine, "E-government Service Adoption by Citizens: A Literature Review and a High-level Model of Influential Factors," *Digital Government: Research and Practice*, vol. 4, no. 1, pp. 2:1–2:24, Apr. 2023.

[8] A. S. Jater, F. Marcus, and I. Pappel, "Comparative Analysis of Youth Engagement and Interest in e-government in the EU," in *2025 International Conference on Next Generation Information System Engineering (NGISE)*, vol. 1, Mar. 2025, pp. 1–6.

[9] N. McDonald and A. Forte, "Privacy and vulnerable populations," in *Modern Socio-Technical Perspectives on Privacy*, B. P. Knijnenburg, X. Page, P. Wisniewski, H. R. Lipford, N. Proferes, and J. Romano, Eds. Cham: Springer International Publishing, 2022, pp. 337–363.

[10] A. Quyoum, M. Wong, S. Ghosh, and S. F. Shahandashti, "Minoritised Ethnic People's Security and Privacy Concerns and Responses towards Essential Online Services," in *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*. Seattle, WA: USENIX Association, Aug. 2025, pp. 259–278.

[11] J. Joffe-Block, "Your data is everywhere. The government is buying it without a warrant ," may 2026. [Online]. Available: https://www.lpm.org/news/2026-03-25/your-data-is-everywhere-the-government-is-buying-it-without-a-warrant

[12] A. M. McDonald, R. W. Reeder, P. G. Kelley, and L. F. Cranor, "A Comparative Study of Online Privacy Policies and Formats," in *Privacy Enhancing Technologies*, I. Goldberg and M. J. Atallah, Eds. Berlin, Heidelberg: Springer, 2009, pp. 37–55.

[13] A. Mhaidli, S. Fidan, A. Doan, G. Herakovic, M. Srinath, L. Matheson, S. Wilson, and F. Schaub, "Researchers' Experiences in Analyzing Privacy Policies: Challenges and Opportunities," *Proceedings on Privacy Enhancing Technologies*, vol. 2023, no. 4, Oct. 2023.

[14] I. Ray, M. K. Wolters, and K. Vaniea, "Why do They Need to Know I Spotted a Pothole? Privacy Issues in Canadian Municipal Problem Reporting Websites," in *Mensch und Computer 2025 - Workshopband*, ser. Mensch und Computer. Gesellschaft für Informatik e.V., 2025.

[15] S. F. King and P. Brown, "Fix my street or else: using the internet to voice local public service concerns," in *Proceedings of the 1st international conference on Theory and practice of electronic governance*. Macao China: ACM, Dec. 2007, pp. 72–80.

[16] K. O'Hara, "Transparency, open data and trust in government: shaping the infosphere," in *Proceedings of the 4th Annual ACM Web Science Conference*, ser. WebSci '12. New York, NY, USA: Association for Computing Machinery, Jun. 2012, pp. 223–232.

[17] P. Matthews, A. Parsons, E. Nyanzu, and A. Rae, "Dog fouling and potholes: understanding the role of coproducing 'citizen sensors' in local governance," *Local Government Studies*, vol. 49, no. 5, pp. 908–931, Sep. 2023, publisher: Routledge.

[18] D. T. O'Brien, D. Offenhuber, J. Baldwin-Philippi, M. Sands, and E. Gordon, "Uncharted Territoriality in Coproduction: The Motivations for 311 Reporting," *Journal of Public Administration Research and Theory*, vol. 27, no. 2, pp. 320–335, Aug. 2016.

[19] "Online profiling: A report to Congress," june 2000. [Online]. Available: https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress-part-2/onlineprofilingreportjune2000.pdf

[20] B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks," in *Proceedings of the 2nd ACM Workshop on Online Social Networks*, ser. WOSN '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 7–12.

[21] B. Krishnamurthy, K. Naryshkin, and C. Wills, "Privacy Leakage vs. Protection Measures: The Growing Disconnect," 05 2012.

[22] Z. Yu, S. Macbeth, K. Modi, and J. M. Pujol, "Tracking the Trackers," in *Proceedings of the 25th International Conference on World Wide Web*, ser. WWW '16. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2016, p. 121–132.

[23] T. Libert, "An Automated Approach to Auditing Disclosure of Third-Party Data Collection in Website Privacy Policies," in *Proceedings of the 2018 World Wide Web Conference*, ser. WWW '18. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2018, p. 207–216.

[24] B. Andow, S. Y. Mahmud, J. Whitaker, W. Enck, B. Reaves, K. Singh, and S. Egelman, "Actions speak louder than words: entity-sensitive privacy policy and data flow analysis with POLICHECK," in *Proceedings of the 29th USENIX Conference on Security Symposium*, ser. SEC'20. USA: USENIX Association, 2020.

[25] S. S. Hashmi, N. Waheed, G. Tangari, M. Ikram, and S. Smith, "Longitudinal compliance analysis of androidapplications with privacy policies," *CoRR*, vol. abs/2106.10035, 2021. [Online]. Available: https://arxiv.org/abs/2106.10035

[26] J. Brookman, P. Rouge, A. Alva, and C. Yeung, "Cross-Device Tracking: Measurement and Disclosures," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, pp. 133–148, 2017.

[27] O. Starov, P. Gill, and N. Nikiforakis, "Are You Sure You Want to Contact Us? Quantifying the Leakage of PII via Website Contact Forms," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, pp. 20–33, 2016.

[28] T. Heino, R. Carlsson, S. Rauti, and V. Leppänen, "Assessing discrepancies between network traffic and privacy policies of public sector web services," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ser. ARES '22. New York, NY, USA: Association for Computing Machinery, 2022.

[29] S. Rauti, R. Carlsson, P. Puhtila, and V. Leppänen, "Third-party data leaks on municipal websites," in *Proceedings of Ninth International Congress on Information and Communication Technology*, X.-S. Yang, S. Sherratt, N. Dey, and A. Joshi, Eds. Singapore: Springer Nature Singapore, 2024, pp. 599–610.

[30] S. Rajapaksha, P. Puhtila, T. Heino, and S. Rauti, "A Comparative Study of Finnish and Sri Lankan Privacy Regulations and Compliance on the Web," in *Proceedings of the 2024 9th International Conference on Information Systems Engineering*, ser. ICISE '24. New York, NY, USA: Association for Computing Machinery, 2025, p. 41–48.

[31] D. Bastos, A. Fernández-Caballero, A. Pereira, and N. P. Rocha, "Smart City Applications to Promote Citizen Participation in City Management and Governance: A Systematic Review," *Informatics*, vol. 9, no. 4, p. 89, Oct. 2022.

[32] V. Diamantopoulou, A. Androutsopoulou, S. Gritzalis, and Y. Charalabidis, "Preserving Digital Privacy in e-Participation Environments: Towards GDPR Compliance," *Information*, vol. 11, no. 2, p. 117, Feb. 2020, number: 2 Publisher: Multidisciplinary Digital Publishing Institute.

[33] C. P. Hoffmann and C. Lutz, "The contextual role of privacy concerns in online political participation," *European Journal of Communication*, vol. 38, no. 4, pp. 363–379, Aug. 2023, publisher: SAGE Publications Ltd.

[34] StatCounter Global Stats, "Browser Market Share Canada," feb 2025. [Online]. Available: https://gs.statcounter.com/browser-market-share/all/canada/#monthly-202502-202603

[35] M. K. Feeney and A. Brown, "Are small cities online? content, ranking, and variation of u.s. municipal websites," *Government Information Quarterly*, vol. 34, no. 1, pp. 62–74, 2017, open Innovation in the Public Sector.

[36] D. L. Wheeler, "zxcvbn: Low-Budget password strength estimation," in *25th USENIX Security Symposium (USENIX Security 16)*. New York, NY, USA: Association for Computing Machinery, 2016, pp. 157–173.

[37] D. Kirkman, K. Vaniea, and D. W. Woods, "Darkdialogs: Automated detection of 10 dark patterns on cookie dialogs," in *Proceedings of the 8th IEEE European Symposium on Security and Privacy (EuroSP'23)*. Los Alamitos, CA, USA: IEEE Computer Society, Jul. 2023, pp. 847–867.

[38] I. Sanchez-Rola, M. Dell'Amico, P. Kotzias, D. Balzarotti, L. Bilge, P.-A. Vervier, and I. Santos, "Can I opt out yet? GDPR and the global illusion of cookie control," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 340–351.

[39] F. Roesner, T. Kohno, and D. Wetherall, "Detecting and defending against Third-Party tracking on the web," in *9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12)*. San Jose, CA: USENIX Association, Apr. 2012, pp. 155–168.

[40] S. Englehardt, D. Reisman, C. Eubank, P. Zimmerman, J. Mayer, A. Narayanan, and E. W. Felten, "Cookies That Give You Away: The Surveillance Implications of Web Tracking," in *Proceedings of the 24th International Conference on World Wide Web*, ser. WWW '15. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2015, p. 289–299.

[41] T. Bujlow, V. Carela-Español, J. Solé-Pareta, and P. Barlet-Ros, "A Survey on Web Tracking: Mechanisms, Implications, and Defenses," *Proceedings of the IEEE*, vol. 105, no. 8, pp. 1476–1510, 2017.

[42] "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content," Jun. 2014. [Online]. Available: RFC7231

[43] I. Fouad, C. Santos, and P. Laperdrix, "The Devil is in the Details: Detection, Measurement and Lawfulness of Server-Side Tracking on the Web," *Proceedings on Privacy Enhancing Technologies*, vol. 2024, pp. 450–465, 10 2024.

[44] DuckDuckGo, "Tracker Radar," 2020, creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. [Online]. Available: https://github.com/duckduckgo/tracker-radar

[45] New Relic, "New Relic network traffic," mar 2025. [Online]. Available: https://docs.newrelic.com/docs/new-relic-solutions/get-started/networks

[46] New Relic, "How to use browser monitoring to improve your website's performance." [Online]. Available: https://docs.newrelic.com/docs/browser/browser-monitoring/getting-started/introduction-browser-monitoring

[47] Microsoft, "Microsoft Defender for Endpoint," may 2026. [Online]. Available: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint

[48] Microsoft, "Microsoft Clarity Documentation," 2026. [Online]. Available: https://learn.microsoft.com/en-us/clarity

[49] Microsoft, "Azure Monitor Overview," 2026. [Online]. Available: https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/overview

[50] Microsoft, "Introduction to Application Insights - OpenTelementry observability," 2026. [Online]. Available: https://learn.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview

[51] E. McCallister, T. Grance, and K. Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," National Institute of Standards and Technology, Tech. Rep. NIST Special Publication 800-122, apr 2010.

[52] S. Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology*, vol. 30, pp. 75–89, 2015.

[53] C. Iorfida, "Canadian sues U.S. Homeland Security, which allegedly sought his Google data after critical social media posts," *CBC News*, May 2026. [Online]. Available: https://www.cbc.ca/news/world/us-dhs-aclu-lawsuit-canadian-john-doe-9.7187851

[54] E. Lev, "'These are real-life consequences': What to know about data sovereignty as the Trump administration tries to unmask an anonymous Canadian," *CTV News*, May 2026. [Online]. Available: https://www.ctvnews.ca/sci-tech/article/these-are-real-life-consequences-what-to-know-about-data-sovereignty-as-the-trump-administration-tries-to-unmask-an-anonymous-canadian

[55] S. Stepanovic, L. Mori, A. Francey, and T. Mettler, "Transparency in Open Government Data Portals: An Assessment of Web Tracking Practices Across Europe," in *Electronic Participation*, M. R. Johannessen, C. Csáki, L. Danneels, S. Hofmann, T. Lampoltshammer, P. Parycek, G. Schwabe, E. Tambouris, and J. Ubacht, Eds. Cham: Springer Nature Switzerland, 2024, pp. 209–222.

[56] S. Ihm and V. S. Pai, "Towards understanding modern web traffic," in *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, ser. IMC '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 295–312.

[57] I. fouad, N. Bielova, A. Legout, and N. Sarafijanovic-Djukic, "Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, pp. 499–518, Apr. 2020.

[58] M. Tahaei and K. Vaniea, ""Developers are Responsible": What Ad Networks Tell Developers About Privacy," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Late Breaking Work*, Apr. 2021, pp. 1–11.

[59] Google Ads Help, "About consent mode." [Online]. Available: https://support.google.com/google-ads/answer/10000067

[60] S. A. Horstmann, S. Domiks, M. Gutfleisch, M. Tran, Y. Acar, V. Moonsamy, and A. Naiakshina, ""Those things are written by lawyers, and programmers are reading that." Mapping the Communication Gap Between Software Developers and Privacy Experts," *Privacy Enhancing Technologies Symposium (PoPETS)*, vol. 2024, pp. 151–170, 2024.

[61] J. R. Reidenberg, J. Bhatia, T. D. Breaux, and T. B. Norton, "Ambiguity in privacy policies and the impact of regulation," *The Journal of Legal Studies*, vol. 45, no. S2, pp. S163–S190, 2016.

[62] A. M. McDonald and L. F. Cranor, "The cost of reading privacy policies," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4, p. 543, 2008.

[63] É. Betters, "Google compiles 60 documents into one privacy policy for 'one Google experience'," Jan. 2012, accessed July 30, 2026. [Online]. Available: https://9to5google.com/2012/01/24/google-compiles-60-documents-into-one-privacy-policy-for-one-google-experience/

[64] "Google product privacy guide," accessed July 30, 2026. [Online]. Available: https://policies.google.com/technologies/product-privacy

APPENDIX

A. Browsing Scenario

In our third scenario, *browsing*, we first visit homedepot.ca, search for "tire gauge", and click on the first result. We next visit usatoday.com, scroll until the "Shopping" header, click on that, and scroll until the "Popular Picks" header. Then we visit expedia.ca, enter "Toronto" in the "Where to?" search field, select "Dates" on the calendar from March 20-27, keep default selection (2 travelers, 1 room) for "Travelers", click "Search", and scroll past 6 results. We then continue to the pothole reporting process as the *regular* scenario (c.f. III-D).