Why do They Need to Know I Spotted a Pothole? Privacy Issues in Canadian Municipal Problem Reporting Websites

Indrani Ray
iray@uwaterloo.ca
University of Waterloo
Waterloo, ON, Canada

Maria Wolters
maria.wolters@offis.de
OFFIS Institute for Information Technology
Oldenburg, Germany

Kami Vaniea
kami.vaniea@uwaterloo.ca
University of Waterloo
Waterloo, ON, Canada

Abstract

Users act as valuable "citizen sensors" by reporting issues in public spaces enabling cities to address infrastructure problems in a timely manner. Municipal web sites are one method for collecting such reports, and they often ask for personal information such as name, phone number, and address in addition to reports. Together with common practices such as third-party connections and the use of cookies, there is the potential for privacy loss, which should be addressed via a clear privacy policy. We examined 14 Canadian Municipal Problem reporting web sites considering issues like what information is required to report, third-party connections, and privacy policies. We checked third-party connections by sampling the web traffic sent when reporting a pothole. We reviewed the 12 cities with a privacy policy and found that coverage varied substantially. For example, five out of 14 cities require personal information to submit a report, but only one has a privacy policy that comprehensively addresses what happens to that data. All city websites contact more third parties during pothole reporting than are mentioned in their privacy policies. Such gaps in privacy policies might negatively affect citizens' trust in the platforms.

CCS Concepts

• **Security and privacy → Privacy protections**; *Social aspects of security and privacy*; • **Human-centered computing → Empirical studies in HCI**.

Keywords

digital participation, e-government, citizen sensing, privacy policies, cookies

1 Introduction

While maintaining infrastructure is the role of municipalities, they often rely on citizens to report problems. In North America, such municipal problem reporting is typically handled through a 311 service, which is a single phone number citizens can call for non-emergency issues. It was introduced to complement the quite effective 911 emergency phone contact line [27]. With the rise of e-government, the 311 reporting infrastructure is now supplemented by online interfaces, which can make reports easier to administer and analyse [8, 17, 27]. Within the context of the United Nations' e-Government statistics, 311 platforms are a form of e-Participation, more specifically e-Consultation [16], where citizens provide municipalities with data about local infrastructure.

Usable privacy that citizens trust is one of the key factors of successful e-Participation [21]. For online 311 systems, this means not just that the system should be secure, it should also protect citizens' personal data, and ensure confidentiality. Crucially, citizens themselves need to be convinced that this is the case. Vulnerable groups that have a vested interest in maintaining their privacy [14] are potentially concerned about the use of their data and may avoid using services that they perceive as being privacy-risky.

While in Germany, and in the EU in general, government web sites are required by law to have a privacy policy, this is not the case in Canada where local government privacy regulations may be delegated at least in part to the Province or Territory. Privacy policies in English 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 [13, 15].

In this study, we review relevant data collection and tracking practices of the online 311 platforms of major Canadian municipalities. By assessing the coverage of privacy policies provided by municipal problem reporting platforms in Canada, we document the information that municipalities provide, and by comparing what is said and what is done, we outline potential case studies for further investigation.

Specifically, we investigate:

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 Does the privacy policy, if it exists, explicitly state the data collected from the user and clearly mention the data collected by third parties?

For the purpose of this initial study, we focus on a single activity that is bound to be covered by all websites, because it matters to everyone living in Canada: the reporting of potholes. Potholes occur throughout the country, reliable information about potholes is

Mensch und Computer 2025 – Workshopband, Gesellschaft für Informatik e.V., 31. August - 03. September 2025, Chemnitz, Germany

https://doi.org/10.18420/muc2025-mci-ws05-350

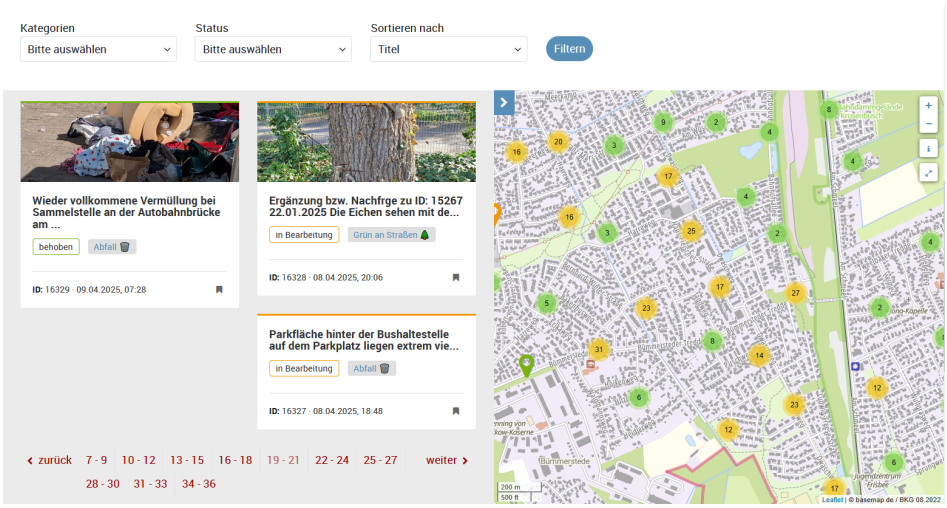


Figure 1: Screenshot of Stadtverbesserer [19], the urban problem reporting system of the city of Oldenburg. Users can search for problems by category and status, browse reported problems, and report new issues. The screenshot reflects the state of Stadtverbesserer on April 9, 2025.

crucial for maintaining municipal road infrastructure, and reporting a pothole should require a minimum of potentially personally identifying information.

2 Related Work

Platforms for reporting infrastructure problems in a municipality come in many different forms. Some platforms, such as the UK's FixMyStreet [10], cover an entire country and forward the reports they receive to municipalities for further processing. Other platforms, such as Boston's comprehensive 311 system, which also provide open data [17], are city-specific.

Figure 1 shows an example of a German municipality-specific website, the city of Oldenburg's Stadtverbesserer (town improver). The start page takes users to an overview of already reported issues, which can be filtered by category (Kategorien) and state of processing (Status) and sorted by date or title. The map shows number of reports per area. Before submitting a report, citizens can check whether the city has already been notified of the issues.

Typically, problem reporting websites use forms with four components: a free text description of the issue, a location (address or pin on a map), a category that describes the type of issue and is often used for internal routing to the correct agency, and an image of the problem.

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. Indeed, data from 311 requests is used by governments to provide evidence of governments doing something about visible issues [8, 18]. Some platforms even require citizens to log in before filing a report in order to reduce spam. Most platforms also allow users to attach photos, which is a popular feature [8]. Photo metadata is not necessarily stripped and can contain details such as geographic location and even author.

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 [12, 20]. Some citizens can even be classified as "superusers" because they contribute a large number of reports [12]. Therefore, attackers can easily profile citizens if they can match their contact information with the reports they submitted. Properly differentiating real citizens from attackers and keeping data collected online safe are ongoing challenges in Canada, as they are world-wide. For example, the Canadian Revenue Agency, which has access to quite sensitive data, continues to battle identity theft and impersonation attacks [4].

To the best of our knowledge, this paper is one of the first systematic attempts to analyse privacy related issues in urban problem reporting systems. While the interplay between privacy and digital participation has received substantial attention [2, 5, 9], we contend that it is important to focus on this specific type of online participation system. Municipal problem reporting done well is an integral component of smart cities. Such systems leverage the power of citizen sensors where expensive sensor technology has not been installed yet and provide important data for digital twins that monitor the state and needs of a municipality.

3 Method

In this study we collect three types of data: potentially identifying data 311 sites ask the user for when reporting, the web connections made when reporting a pothole, and the privacy policy.

3.1 City selection

We chose 14 Canadian cities to evaluate using the following criteria. We started with a list of all Canadian cities with populations above 100,000 according to the 2021 Canadian Census [3]. For each each Province/Territory that was not yet included, we included the largest municipality or city that had a 311 website. We include municipalities as well as cities because due to Canada's geography

Table 1: PII collected via the UI during a pothole service request.

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

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

some cities join together into larger municipalities to handle infrastructure issues. Prince Edward Island has no municipality with a 311 website, and is therefore not represented. The result was the 14 municipalities listed in Table 1.

We decided to focus on larger cities/municipalities for two reasons. First they represent a large proportion of the Canadian population. Second, larger cities are known to be earlier adopters of digitalisation than smaller cities [7].

3.2 Personal information requested by websites

To scope the project, we decided to limit our analysis to services related to broken or otherwise not functioning infrastructure services. This excluded services like park shelter rentals and interactions with coyotes.

We took a bottom-up approach to identify potential personal information. The lead researcher recorded all the information types requested by Toronto – which has one of the most comprehensive 311 sites – and reviewed the list with another researcher. The data types in Table 2 were identified as potentially identifying as they involve the person's name, contact information, or physical location. We also include attachments as photo attachments can contain personal information either in the photo or via embedded data like GPS. "Details" were often asked for. We include them as potentially identifying as the person may choose to include more information such as their contact information or their name. When problem reports are published online as part of transparent open data initiatives (e.g. [18]), such personal data is not systematically removed. Such editing requires time and effort, and municipalities argue that it is ultimately citizens' responsibility to check information that will be made publicly available online. The list of PII was revisited several times during data collection, but only minor adjustments to codebook definitions were required.

3.3 Pothole reporting: third parties contacted

We specifically focus on the ever-present potholes, which appear throughout Canada even in the summer. Therefore, they are well covered in municipal problem reporting web sites and are an issue that people living in Canada care about deeply. We also find that the submission form for potholes often uses the same website and general website-flow as other service issues, so we anticipate that data collected during pothole reporting is quite similar to other services. The name of pothole-related service requests varied by municipality. Options included Pothole(s), Pothole on the Roadway, Pothole Repair, Report a Pothole, Report a Pothole or Sinkhole, Road Pothole, Road Damage, and Road Maintenance.

For each city, we record an HTTP Archive (HAR) file while entering a pothole service request starting from the city's 311 homepage up until the form submission button, but not submitting. We only supply information necessary to enable submission — only entering data in fields that are explicitly marked as required or otherwise indicated as mandatory by the interface. The data collection was done via the official 64-bit build Google Chrome, version 137.0.7151.119, on an Ubuntu 24.04.2 LTS laptop physically located in Ontario Canada and therefore with a Canada-associated IP address. Before each pothole request, we 'delete browsing data from all time' which, according to Google Chrome settings, deletes browsing history, downloaded history, cookies and other site data, cached images and files, passwords and other sign-in data, autofill form data, site settings, and hosted app data.

To analyse HAR files, we used a Python script to extract the third-party domains as well as the query strings, post data, and cookies. We focus on GET requests and cookie data as these are easiest to parse. We visually scanned the key-value pairs for obviously personal information such as phone numbers or postal addresses.

Third-party trackers often use unique alphanumeric strings that resemble globally unique identifiers (GUID). These identifiers are used to uniquely identify and therefore track users. If 311 sites are sending such ID-like values to third-party sites, it could be privacy-problematic. One proposed approach to identifying such ID-like variables at scale is to use the `zxcvbn` password strength algorithm [26] to calculate entropies of the data values. Truly random numbers naturally have high entropy and a password calculation is

an easy way to find them. ID-like cookies and GET variables have been used in prior third-party tracking research successfully [11, 24] and the threshold entropy level of 3 has been shown to work well. We therefore extracted all key value pairs from GET and from cookies and computed the entropy using `zxcvbn` and marked any pair with an entropy of 3 or more as ID-like. We also manually reviewed portions of the data and find that the approach works well to find likely ID-like values.

3.4 Privacy policies

While collecting data from the 311 websites we also recorded the URL and downloaded an offline PDF of their associated privacy policy. For 11 cities, links to the privacy policy was accessible from the footer of the service request pages. The city of Yellowknife has a privacy policy, but the domain through which online services are reported does not contain any mention or link to it, so we located it by searching. The cities of Whitehorse and Iqaluit do not have privacy policies although the website for the former contains a footer with the words 'Privacy Policy' without a link.

We inspected privacy policies for sentences that mention the collection, retention, share, and use of information. We use the term 'information' here to broadly encompass three categories as per the language of the privacy policies: personal information, device information, and information provided by visitors to the city's page either directly through explicit correspondence or implicitly collected by web servers.

We also scanned each city's privacy policy for explicitly-named third-parties and whether or not they collect additional data for analytical or statistical purposes.

4 Results

4.1 Personal information requested (RQ1)

Table 1 contains the PII collected by each city's UI when a citizen requests a pothole to be filled. Although the cities were divided on whether or not they require citizens to provide explicit personal information, such as name and phone number, the majority required information that could be potentially personally identifiable, such as the location of the infrastructure issue, and encouraged or required submission of further details.

4.2 Third-party connections (RQ2)

Modern websites are often composed of elements from multiple domains normally to speed development and to track visitors. For example, `fonts.gstatic.com` is commonly used by websites who are using Google's free font library. While such connections are common, each connection does send basic data to the remote third-party server such as the IP address, browser type, and operating system version. Some third-party sites also use cookies to store unique identifiers allowing for tracking across multiple pages.

We recorded all the connections that occurred while reporting a pothole. All municipal 311-sites contacted third parties, and all but three of them contacted at least one known analytics or tracking provider. Google Analytics was the most common analytics used. The remaining three municipalities made use of other Google services like Maps and Gstatic – a content delivery network for static resources provided by Google.

We further looked at all connections to find ID-like values in cookies and GET strings. We found a total of 54 unique id-like cookies across all cities. Out of the top ten most frequently contacted third parties from all pothole requests, only `www.google.com` is found to be setting id-like cookies for multiple cities, followed by `googleads.g.doublick.net` which sets id-like cookies for two cities as shown in Table 3. The most popular cookie name across several cities, `_GRECAPTCHA`, is used for Google's reCAPTCHA service and other popular cookie names such as `BrowserId` and `MUID` are explicitly for user identification. Another frequently used cookie was `AGS_ROLES`, which is generated by the geoinformation system ArcGIS for interactive services. The most common first-party cookie name we observed is `_ga` which appears for nine cities and according to Google's Analytics Help page is "Used to distinguish users"[1].

We find 85 unique city-to-third-party-domain connection pairs that contained at least one id-like value. In total, we observed 929 id-like values being sent. The most popular ID-like query string keys `tid`, `tag_exp`, `gcd`, `td`, `dl`, `cid`, and `gtm` are related to Google Services, particularly Google Analytics and Google Tag Manager. These are the most common because they were all present in requests made across eleven cities. In our analysis, we find St. John's to be a unique case in that all the requests with ID-like query string values are from the same domain:
`stjohns.form.ca.empro.verintcloudservices.com`.
Surprisingly, Yellowknife has no third-party requests with ID-like values.

4.3 Privacy policies (RQ3)

Six cities (43%) provided information about how and for what purpose data was being collected in the submission user interface itself (Figure 2). The contents of these declarations ranged from mentioning municipal acts by which cities can collect information, to presenting links to respective privacy policies, to requiring user consent as shown in Figure 2c. Eleven cities (79%) provided links to privacy policies that were accessible from footers of service request pages. The linked privacy policies all covered the entire municipal web site and were not specific to the 311 platform.

All cities with a privacy policy mentioned the collection of information. Cities either explicitly claim to collect personal information or, more frequently, claim that they only do so when the information is voluntarily provided by visitors (and not automatically). The city of Saskatoon is a good example:

> *The City of Saskatoon does not gather any personal information while you browse our website. Some personal information, including, but not limited to; name and email address may be voluntarily provided by users of this site to request services such as; newsletter sign up, image download, online surveys and other similar services.*

The personal information mentioned the most frequently in privacy policies are name and email followed by address then phone number. Quite a few policies mention cookies and reference collecting IP information; however, policies vary in their characterization of data collected or cookie purposes. An overview of information collected as presented in privacy policies is given in Table 2.

Table 2: Information explicitly mentioned in privacy policies. Note that many privacy policies use general terms like "personal information" which is not represented in this table.

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

With the exceptions of Toronto and Moncton, all cities' privacy policies contain statements pertaining to sharing personal information. Eight cities clearly state that they do not sell, share, rent, disclose, or exchange personal information with third parties, those outside of the organization, or authorities unless required by law. The remaining cities are less explicit about not sharing. Two cities roughly state that PI is used for the purpose for which it was given. Montreal, on the other hand, asserts that "the city has the right to use or disclose requests for any reason whatsoever."

When we compare the information that is required for reporting a pothole (c.f. Table 1) to the information that is explicitly covered by the privacy policy (c.f. Table 2), only one city explicitly mentions name, email, phone, and address, which fall under the classic, narrow definition of PII, even though five cities require all of this information. No city explicitly mentions all of the required potential PII, such as location, attachment, or details. Cities though are making more general statements about PII collection. Six out of fourteen cities (43%) say that they collect personal information and give some examples. Two (14%) mention "personal information" without defining the term, and four (29%) use general statements like "contact information".

We searched all privacy policies for the third parties that we most commonly observed while reporting a pothole. We found that some but not all policies disclosed that they use third-party services to collect analytics (c.f. Table 4). Ottawa's policy mentions that their website uses Google Analytics which transmits information to their servers. Winnipeg's policy mentions the usage of third-party service Google Analytics (which collects device information) and Google reCAPTCHA (which the policy says transmits information to Google). Halifax's policy also adds that device information may be collected by "third-party service providers such as Google, Browse Aloud, AddThis and other plugins and social media widgets." Montreal's policy mentions that data collected by Google Analytics may be transmitted outside Canada and that the city uses an external application for user feedback on the website.

Table 4 compares the number of third parties mentioned in the privacy policies to the number of unique third parties contacted during a pothole request. Here we are looking at any connection that contacts a different domain than the main 311 website. For all cities, we found more unique third parties during the request than were mentioned in the privacy policy. However, it can be challenging to accurately judge if a third-party domain is a privacy concern or not. Many websites, for example, use content management systems which improve content delivery speed but are not necessarily a privacy risk.

To more accurately look at potentially privacy-risky connections, we limit our analysis of third-party contacts to those connections that involve an id-like value in a cookie or in the GET string as these are more likely to be tracking and therefore privacy-concerning [11].

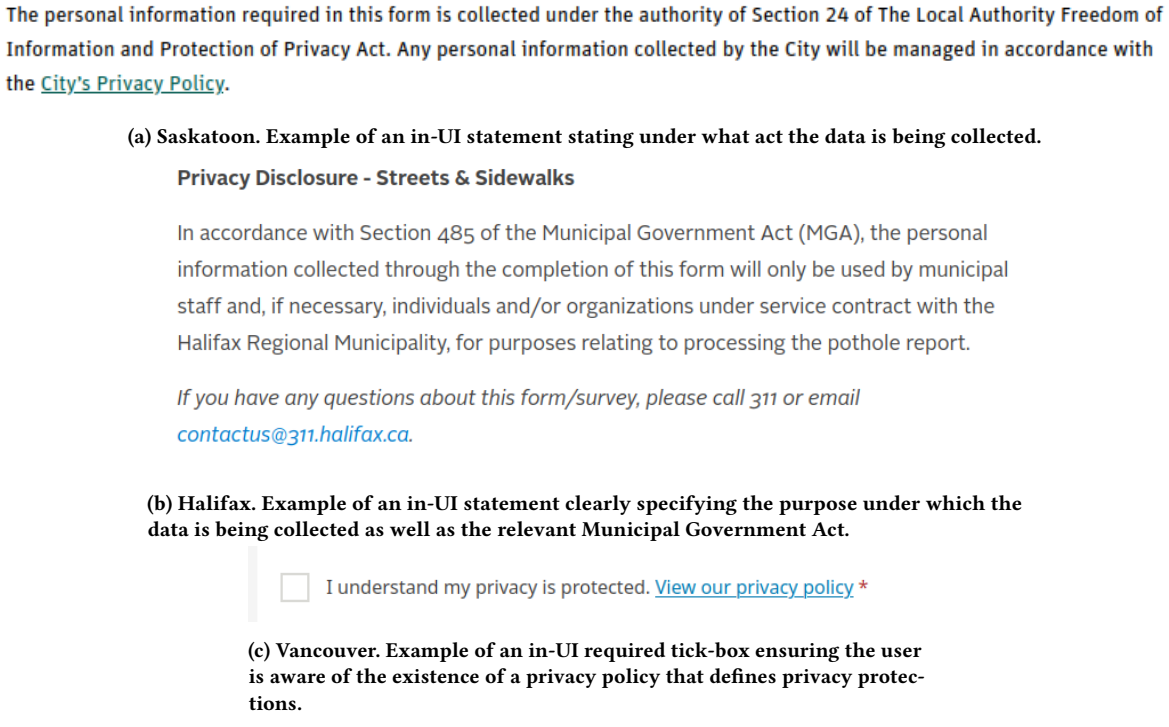
The cities of St. John's, Vancouver, and Yellowknife do not explicitly mention collecting user data for analytical or statistical purposes (as shown in Table 4) though the city of Yellowknife claims to collect and store device information to make the site more

Table 3: Cookies set by or sent to third parties.

	c.bing.com	c.clarity.ms	d.la1-c2-ia4.salesforceliveagent.com	googleads.g.doubleclick.net	maps.ottawa.ca	maps.vancouver.ca	o.clarity.ms	service.force.com	stjohns.form.ca.empro.verintcloudservices.com	syndication.twitter.com	td.doubleclick.net	translate-pa.googleapis.com	www.clarity.ms	www.google.com	www.youtube.com
Calgary															
Halifax				✓							✓			✓	✓
Iqaluit		✓					✓						✓	✓	
Moncton															
Montreal	✓	✓											✓	✓	
Ottawa					✓										
Saskatoon															
St. John's									✓						
Toronto			✓					✓				✓		✓	
Vancouver						✓					✓				
Waterloo										✓	✓	✓			
Whitehorse				✓						✓	✓			✓	
Winnipeg															
Yellowknife															

Table 4: Counts of unique third parties: named in privacy policies, contacted during pothole service request process, and using ID-like values in cookies or GET strings, as well as if the privacy policy mentions analytics at all.

City	Third party Mentioned	Third party Contacted	Third party Using ID-like Values	Analytics Mentioned
Calgary	0	6	4	✓
Halifax	3	9	7	✓
Iqaluit	-	9	4	NA
Moncton	0	8	4	✓
Montreal	1	18	9	✓
Ottawa	1	11	6	✓
Saskatoon	0	10	3	✓
St. John's	0	8	1	-
Toronto	0	19	7	✓
Vancouver	0	17	10	-
Waterloo	2	23	16	✓
Whitehorse	-	20	12	NA
Winnipeg	3	12	4	✓
Yellowknife	0	7	0	-



(a) Saskatoon. Example of an in-UI statement stating under what act the data is being collected.

(b) Halifax. Example of an in-UI statement clearly specifying the purpose under which the data is being collected as well as the relevant Municipal Government Act.

(c) Vancouver. Example of an in-UI required tick-box ensuring the user is aware of the existence of a privacy policy that defines privacy protections.

Figure 2: Mentions of privacy policies and privacy disclosures in the user interface.

useful to visitors and to learn about the number of visitors and types of technology they use.

5 Discussion and Conclusion

We surveyed the municipal problem reporting web sites of all Canadian cities with more than 100,000 inhabitants and the largest municipalities in provinces or territories where no city with more than 100,000 inhabitants exists, except for Prince Edward Island. We focused on data automatically being collected during pothole reporting, a functionality that is crucial for road infrastructure. Our methodology can be used to systematically uncover privacy related issues relevant to digital municipal problem reporting solutions. Our data collection is underpinned by procedures and data structures that can be easily ported to other countries, including the EU.

Regarding RQ1, we found that nine out of fourteen (64%) municipalities only require potential PII, such as location, while five (26%) also require users to provide PII that fits the classic definition, such as name, email, address, or phone number. While this data is potentially privacy-sensitive, it is also being collected with a clear purpose, namely collecting specifics about the issue and contacting the original issue reporter if more clarification is needed. We were pleased to see that cities are not collecting PII beyond what would make sense for the interaction and that two thirds of cities give the user the option to only provide data about the issue and omit their own contact information. That said, privacy policies were often in reference to a whole city rather than one specific service, so we unsurprisingly find that most privacy policies make general statements about city-wide data usage and do not clearly state how data collected by the 311-service page will be used.

When reporting a pothole (RQ2), a median of 10.5 third parties were contacted, and many query strings included ID-like values. The privacy policies, if they exist, do not explicitly list all of the PII collected, and mention far fewer third parties than we observed (RQ3). A user trying to understand how such connections are governed would not find sufficient information in the privacy policy. While we expect that most Canadian cities do aim to protect citizen privacy, there is still ample opportunity for expectation misalignment between citizen's expectations and how the page actually operates.

The numerous issues we found resonate with the findings of Drescher et al. [6], who examined apps provided by German cities. While Drescher et al. proceeded to notify app developers of their findings, and tested the effectiveness of different ways of wording those notifications in the process, we chose not to contact the Canadian municipalities whose web sites we investigated. As outlined in Section 1, in Canada, there is a complex interplay between federal and provincial laws and regulations that may require additional collaboration in future work to accurately unpick.

Instead, this work provides an initial investigation into issues that might affect citizen's trust in 311 platforms, and by extension their willingness to report issues. There are two main aspects here: trust that the problem reports will be acted on, and trust that personally identifying information such as contact data will be kept confidential. To the best of our knowledge, there has been no specific research on this issue. Following the trust framework outlined

by Riegelsberger et al. [23], we would assume that the key factor will be institutional, i.e. trust in government services. A recent review focusing on data from 2022–2023 reported that only 51% of Canadians trust government institutions in general [25].

Finally, in future work we aim to extend this methodology to the context of Germany and the EU, where regulations are substantially more strict. An initial analysis we conducted of privacy and data protection policies of five major German cities with more than 100,000 inhabitants [22] yielded similar results to Table 2, with substantial variation in the information mentioned. It remains to be seen what happens when we make and track pothole reports.

Acknowledgments

Maria 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] Google Analytics. [n. d.]. Dimentions and metrics: [GA4] Cookie usage on websites. https://support.google.com/analytics/answer/11397207?hl=en Accessed July 31, 2025..

[2] David Bastos, Antonio Fernández-Caballero, António Pereira, and Nelson Pacheco Rocha. 2022. Smart City Applications to Promote Citizen Participation in City Management and Governance: A Systematic Review. *Informatics* 9, 4 (Oct. 2022), 89. https://doi.org/10.3390/informatics9040089

[3] Statistics Canada. 2023. Census Profile, 2021 Census of Population. https://www12.statcan.gc.ca/census-recensement/2021/dp-pd/prof/index.cfm

[4] Harvey Cashore, Eva Uguen-Csenge, and Mark Kelly. 2025. Who's hacking CRA accounts? https://www.cbc.ca/newsinteractives/features/whos-hacking-cra-accounts

[5] Vasiliki Diamantopoulou, Aggeliki Androutsopoulou, Stefanos Gritzalis, and Yannis Charalabidis. 2020. Preserving Digital Privacy in e-Participation Environments: Towards GDPR Compliance. *Information* 11, 2 (Feb. 2020), 117. https://doi.org/10.3390/info11020117 Number: 2 Publisher: Multidisciplinary Digital Publishing Institute.

[6] Jan Niklas Drescher, Jakob Moser, Nicolas Strangmann, Jonas Spinner, Dominik Herrmann, and Melanie Volkamer. 2024. "Data Protection Can Sometimes Be a Nuisance" A Notification Study on Data Sharing Practices in City Apps. In *Mensch und Computer 2024 - Workshopband*. Gesellschaft für Informatik e.V., 10.18420/muc2024. https://dl.gi.de/handle/20.500.12116/44292

[7] Mary K. Feeney and Adrian Brown. 2017. Are small cities online? Content, ranking, and variation of U.S. municipal websites. *Government Information Quarterly* 34, 1 (2017), 62–74. https://doi.org/10.1016/j.giq.2016.10.005 Open Innovation in the Public Sector.

[8] Sarah Hartmann, Agnes Mainka, and Wolfgang G. Stock. 2017. Citizen Relationship Management in Local Governments: The Potential of 311 for Public Service Delivery. In *Beyond Bureaucracy: Towards Sustainable Governance Informatisation*, Alois A. Paulin, Leonidas G. Anthopoulos, and Christopher G. Reddick (Eds.). Springer International Publishing, Cham, 337–353. https://doi.org/10.1007/978-3-319-54142-6_18

[9] Christian Pieter Hoffmann and Christoph Lutz. 2023. The contextual role of privacy concerns in online political participation. *European Journal of Communication* 38, 4 (Aug. 2023), 363–379. https://doi.org/10.1177/02673231221139040 Publisher: SAGE Publications Ltd.

[10] Stephen F. King and Paul Brown. 2007. 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*. ACM, Macao China, 72–80. https://doi.org/10.1145/1328057.1328076

[11] Daniel Kirkman, Kami Vaniea, and Daniel W. Woods. 2023. DarkDialogs: Automated detection of 10 dark patterns on cookie dialogs. In *Proceedings of the 8th IEEE European Symposium on Security and Privacy (EuroSP'23)*. IEEE Computer Society, Los Alamitos, CA, USA, 847–867. https://doi.org/10.1109/EuroSP57164.2023.00055

[12] Peter Matthews, Alex Parsons, Elvis Nyanzu, and Alasdair Rae. 2023. Dog fouling and potholes: understanding the role of coproducing 'citizen sensors' in local governance. *Local Government Studies* 49, 5 (Sept. 2023), 908–931. https://www.tandfonline.com/doi/abs/10.1080/03003930.2022.2116575 Publisher: Routledge.

[13] Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor. 2009. A Comparative Study of Online Privacy Policies and Formats. In *Privacy Enhancing Technologies*, Ian Goldberg and Mikhail J. Atallah (Eds.). Springer, Berlin, Heidelberg, 37–55. https://doi.org/10.1007/978-3-642-03168-7_3

[14] Nora McDonald and Andrea Forte. 2022. Privacy and Vulnerable Populations. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing, Cham, 337–363. https://doi.org/10.1007/978-3-030-82786-1_15

[15] Abraham Mhaidli, Selin Fidan, An Doan, Gina Herakovic, Mukund Srinath, Lee Matheson, Shomir Wilson, and Florian Schaub. 2023. Researchers' Experiences in Analyzing Privacy Policies: Challenges and Opportunities. *Proceedings on Privacy Enhancing Technologies* 2023, 4 (Oct. 2023). https://doi.org/10.56553/popets-2023-0111

[16] United Nations. [n. d.]. E-Participation Index. https://publicadministration.un.org/egovkb/en-us/About/Overview/E-Participation-Index

[17] Daniel Tumminelli O'Brien. 2016. Using small data to interpret big data: 311 reports as individual contributions to informal social control in urban neighborhoods. *Social Science Research* 59 (Sept. 2016), 83–96. https://doi.org/10.1016/j.ssresearch.2016.04.009

[18] Kieron O'Hara. 2012. Transparency, open data and trust in government: shaping the infosphere. In *Proceedings of the 4th Annual ACM Web Science Conference (WebSci '12)*. Association for Computing Machinery, New York, NY, USA, 223–232. https://doi.org/10.1145/2380718.2380747

[19] Stadt Oldenburg. [n. d.]. *Stadtverbesserer*. https://gemeinsam.oldenburg.de/de/stadtverbesserer last retrieved: July 18, 2025.

[20] Daniel Tumminelli O'Brien, Dietmar Offenhuber, Jessica Baldwin-Philippi, Melissa Sands, and Eric Gordon. 2017. Uncharted Territoriality in Coproduction: The Motivations for 311 Reporting. *Journal of Public Administration Research and Theory* 27, 2 (April 2017), 320–335. https://doi.org/10.1093/jopart/muw046

[21] Eleni Panopoulou, Efthimios Tambouris, and Konstantinos Tarabanis. 2014. Success factors in designing eParticipation initiatives. *Information and Organization* 24, 4 (2014), 195 – 213. https://doi.org/10.1016/j.infoandorg.2014.08.001

[22] Fynn-Benno Prusch. 2025. *Automatisierte Auswertung von Datenschutzerklärungen anhand von Mängelmeldern*. Bachelor Thesis. Carl-von-Ossietzky Universität Oldenburg, Oldenburg.

[23] Jens Riegelsberger, M. Angela Sasse, and John D. McCarthy. 2005. The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies* 62, 3 (2005), 381–422. https://doi.org/10.1016/j.ijhcs.2005.01.001

[24] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. 2019. 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*. Association for Computing Machinery, New York, NY, USA, 340–351.

[25] J Steinburg. 2024. *Trust in Canada: Recent Trends in Measures of Trust*. Technical Report. Trust in Research Undertaken in Science and Technology (TRuST) Scholarly Network, University of Waterloo.

[26] Daniel Lowe Wheeler. 2016. zxcvbn: Low-Budget password strength estimation. In *25th USENIX Security Symposium (USENIX Security 16)*. Association for Computing Machinery, New York, NY, USA, 157–173.

[27] Ariel White and Kris-Stella Trump. 2018. The Promises and Pitfalls of 311 Data. *Urban Affairs Review* 54, 4 (July 2018), 794–823. https://doi.org/10.1177/1078087416673202 Publisher: SAGE Publications Inc.