A LARGE-SCALE EVALUATION OF PRIVACY PRACTICES OF PUBLIC WIFI CAPTIVE PORTALS

SUZAN ALI AHMAD ALI

A THESIS

IN

THE DEPARTMENT OF

CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING

PRESENTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF MASTER OF APPLIED SCIENCE

IN INFORMATION SYSTEMS SECURITY

CONCORDIA UNIVERSITY

MONTRÉAL, QUÉBEC, CANADA

AUGUST 2020

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Suzan Ali Ahmad Ali**

Entitled: **A Large-scale Evaluation of Privacy Practices of Public WiFi Captive Portals**

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science
in Information Systems Security

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Chair
Dr. Walter Lucia

_____ Examiner
Dr. Jeremy Clark

_____ External Examiner
Dr. M. Zahangir Kabir

_____ Supervisor
Dr. Mohammad Mannan and Dr. Amr Youssef

Approved by _____
Dr. Mohammad Mannan, Graduate Program Director

May 25, 2020 _____

Dr. Mourad Debbabi, Interim Dean
Gina Cody School of Engineering and Computer Science

ABSTRACT

A Large-scale Evaluation of Privacy Practices of Public WiFi Captive Portals

Suzan Ali Ahmad Ali

Open access WiFi hotspots are widely deployed in many public places, including restaurants, parks, coffee shops, shopping malls, trains, airports, hotels, and libraries. While these hotspots provide an attractive option to stay connected, they may pose security and privacy risks to users. Several past studies focused on privacy leakage from browsing the internet or using mobile apps in an open hotspot, due to the nature of these hotspots, and the use of HTTP, as opposed to HTTPS for connections between the user device and the web service. The US Federal Trade Commission (FTC) acknowledges those risks and advises public WiFi users to take reasonable measures while using such networks.

To complement previous efforts in analyzing security and privacy risks of using public WiFi hotspots, we design two comprehensive frameworks. The first framework (`CPInspector`) is designed to analyze the tracking behaviors and privacy leakage on public WiFi captive portals—where users typically agree to the hotspot's terms or sometimes register before being allowed to access the internet. CPInspector performs a wide range of web tracking measurements on public WiFi captive portals for both Windows and

Android; we must physically visit each hotspot and run the CPInspector on the hotspot captive portal. We also inspect the personal data collection practices of those hotspots and the security measures adopted to protect users' information. Hotspots pose some unique risks due to their access to the users' foot traffic, browsing habits, the device MAC address, and in certain cases, personal information such as name, email address, social media profile, location and employment history. Using CPInspector, we initially conducted a comprehensive privacy analysis of 80 public WiFi hotspot locations in Montreal, Canada. Our analysis reveals the collection of a significant amount of privacy-sensitive personal data through the use of social login (e.g., Facebook and Google) and registration forms, and many instances of tracking activities, sometimes even before the user accepts the hotspot's privacy and terms of service policies. We also analyzed 98 hotspot locations in Montreal for ad injection, but we did not observe any content modification attempts. Next, we expanded our study to hotspots from other cities in Canada, Europe, and the US. We conducted a high-level comparative analysis of tracking behaviors of those hotspots (in total, 192 public WiFi hotspot locations; including Montreal hotspots). We conclude that some of our findings are indeed applicable to a larger geographical area, including the use of third-party trackers on captive portals and sharing the harvested data with third-party entities using third-party captive portals.

We use the second framework to analyze hotspots privacy policies and terms-of-use documentation which also discloses the service provider's data and privacy practices. We augment our policy analysis using our collected hotspots' datasets to validate selected privacy aspects of the public WiFi. We evaluated a sample of 16 privacy policy and TOS

documents from hotspots that appear to be most risky in Montreal, Canada. Our analysis reveals many instances where the hotspot may appear to conform to privacy best practices according to its documentation but fail to implement necessary technical measures.

Acknowledgments

I would like to thank my supervisors, Dr. Mohammad Mannan and Dr. Amr Youssef for giving me the opportunity to work under their supervision. Their continued support have been invaluable throughout every stage of my research. I would also like to express my gratitude for their patience, motivation, enthusiasm and immense knowledge. I am incredibly lucky to have two advisors who inspired me with bright ideas, helpful comments, suggestions, and insights which have contributed to the improvement of this work.

Special thanks to all professors at CIISE. They all provided me with the opportunity to learn in a positive learning environment and made me more and more interested in all aspects of systems security. I would like to express my special gratitude to Dr. Ayda Basyouni for her continued assistance and advice. I would also like to thank the members of Concordia's Madiba Security Research Group for their support and inspiring discussions.

I received substantial financial support from several sources including: Pierre Harbor Foundation Scholarship and Concordia University. This work was partly supported by a grant from the Office of the Privacy Commissioner of Canada (OPC) Contributions Program. I am thankful to all for easing the financial burden while doing this research.

Lastly, I would like to thank my family and friends. This journey would not have

been possible without their encouragement and support. I owe thanks to a very special person, my husband, Dr. Walid Alqaisi for his continued and unfailing love, support, and understanding during my pursuit of master degree that made the completion of this thesis possible. You are the reason I accomplish this today. I greatly value your contribution and deeply appreciate your belief in me. I also dedicate this thesis to my five lovely children, Tameem, Julianna, Aous, Rakan, and Sarah who are the pride and joy of my life. I love you more than anything and I appreciate all your patience and support during my study.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

Public WiFi hotspots are growing in popularity across the globe. Most users frequently connect to hotspots due to their free-of-cost service, (as opposed to mobile data connections) and ubiquity. According to a Symantec study [56] conducted among 15,532 users across 15 global markets, 46% of participants do not wait more than a few minutes before connecting to a WiFi network after arriving at an airport, restaurant, shopping mall, hotel or similar locations. Furthermore, 60% of the participants are unaware of any risks associated with using an untrusted network, and feel their personal information is safe.

A hotspot may have a captive portal, which is usually used to communicate the hotspot's privacy and terms-of-service (TOS) policies, and collect personal identification information such as name and email for future communications, and authentication if needed (e.g., by asking the user to login to their social media sites). Upon acceptance of the hotspot's policy,

the user is connected to the internet and her web browser is often automatically directed to load a landing page (usually the service provider's webpage).

Several past studies (e.g., [13, 54]) focused on privacy leakage from browsing the internet or using mobile apps in an open hotspot, due to the lack of encryption, e.g., no WPA/WPA2 support at the hotspot, and the use of HTTP, as opposed to HTTPS for connections between the user device and the web service. However, in recent years, HTTPS adoption across web servers has increased dramatically, mitigating privacy exposure through plain network traffic. For example, according to the Google Transparency Report [26], as of April 6, 2019, 82% of web pages are served via HTTPS for Chrome users on Windows. On the other hand, in the recent years, there have also been several comprehensive studies on web tracking on regular web services and mobile apps with an emphasis on most popular domains/services (see e.g., [9, 10, 21]).

In contrast to past hotspot and web privacy measurement studies, we analyze tracking behaviors and privacy leakage in WiFi captive portals and landing pages. We design a data collection framework (`CPInspector`) for both Windows and Android, and capture raw traffic traces from several public WiFi that require users to go through a captive portal before allowing internet access. Challenges here include: manual collection of captive portal data by physically visiting each hotspot; making our test environment separate from the regular user environment so that we do not affect the user's browsing profiles; ensuring that our tests remain unaffected by the user's past browsing behaviors (e.g., saved tracking cookies); and creating and monitoring several test accounts in popular social media or email services as some hotspots mandate such authentication.

From each hotspot evaluated in Montreal (Canada), we collect traffic using both Chrome and Firefox on Windows. In addition to the default browsing mode, we also use private browsing, and deploy two ad-blockers to check if such privacy-friendly environments help against captive portal trackers—leading to a total of eight datasets for each hotspot. We also use social logins (Facebook, LinkedIn, Google, Instagram, Twitter) if required by the captive portal, or provided as an option; we again use both browsers for social login tests (two to six additional datasets as we have observed at most three social login options per hotspot). Some hotspots also require the user to complete a registration form that collects the user's PII—in such cases, we collect two more datasets (from both browsers). Finally, some hotspots collect additional personal information as part of an optional survey. When reporting statistics on tracking domains and cookies, we accumulate the *distinct* trackers as observed in all the datasets collected for a given hotspot.

On Android, we collect traffic only from the custom captive portal app (as opposed to Chrome/Firefox on Windows) as the cookie store of this app is separate from browsers. Consequently, tracking cookies from the Android captive portal app cannot be used by websites loaded in a browser. Recent Android OSes also use dynamic MAC addresses, limiting MAC address-based tracking. However, we found that cookies in the captive portal app may remain valid for up to 20 years, allowing effective tracking by hotspot providers.

Note: *by default, all our statistics refer to the measurements on Windows; we explicitly mention when results are for Android (mostly in Sec.3.2).*

1.2 Contributions

Our contributions can be summarized as follows:

1. We design, develop, and implement a framework (`CPInspector`)[1] that perform a wide range of web tracking measurements on public WiFi captive portal for both Windows and Android. Using our framework, we conducted two phases of data collection and analysis of public WiFi hotspots. First, we collected data from 80 hotspot locations in Montreal (Quebec), Canada. Then we extended our data collection to a wider geographical area, including other cities in Canada, Europe and the US. In total, we collected and analyzed 192 public WiFi hotspot locations, making this the largest such study to characterize hotspots in terms of their privacy risks.

2. In phase one, we collected a total of 679 datasets from the captive portal and landing page of 80 hotspot locations in Montreal, Canada between September 2018 to April 2019. We analyzed over 18.5GB of collected traffic for privacy exposure and tracking, and report the results from 67 unique hotspots. We show the collection of a significant amount of privacy-sensitive personal data through the use of social login (e.g., Facebook and Google) and registration forms, and many instances of tracking activities, sometimes even before the user accepts the hotspot's privacy and terms of service policies. Most hotspots use persistent third-party tracking cookies within their captive portal site; these cookies can be used to follow the user's browsing behavior long after the user leaves the hotspots, e.g., up to 20 years. Moreover, several

[1] https://github.com/MadibaLab/CPInspector

hotspots explicitly share (sometimes via HTTP) the collected personal and unique device information with many third-party tracking domains. Additionally, from our Android experiments, we reveal that hotspots can effectively track Android devices even though Android uses a separate captive portal app and randomizes MAC address as visible to the hotspot.

3. We also design our framework to detect ad/content injection by hotspots. We collected over 8.7GB traffic (346 datasets) by crawling two honey websites and BBC.com from 98 hotspot locations (hotspots without captive portals are also included). We did not observe any content modification attempts by the hotspots.

4. In phase two, we collected a total of 130 datasets from the captive portal and landing page of 112 hotspot locations in Ontario (39; Canada), Luxembourg (43; Europe), Netherlands (3; Europe), France (2; Europe), and New York (25, USA) between July 2019 to October 2019.[2] We conducted a high-level comparative analysis of tracking behaviors of those hotspots (in total, 192 public WiFi hotspot locations; including Montreal hotspots). We conclude that some of our reported findings, from phase one, are applicable to a larger geographical area including, the use of third-party trackers on captive portals and sharing the harvested data with third-party entities through the use third-party captive portal.

5. Finally, we propose a framework to analyze hotspots privacy policies and terms-of-use documentation. We augment our policy analysis by the use of our collected

[2]We stopped collecting datasets from Firefox as the collected datasets were largely the same. We also stopped collecting datasets in private browsing, ad-blockers, and Android as the focus in this phase is to compare tracking behaviors between hotspots in Europe, Canada, and the US.

hotspots' datasets to validate some of those privacy practices. We evaluated a sample of 16 privacy policy and TOS documents from hotspots that appear to be most risky in Montreal, Canada. Our analysis reveals many instances where the hotspot may appear to conform to privacy best practices according to its documentation. but fail to implement necessary technical measures.

Some of the work discussed in this dissertation has been peer-reviewed and published in the following article: Suzan Ali, Tousif Osman, Mohammad Mannan and Amr Youssef. On Privacy Risks of Public WiFi Captive Portals. Workshop on Data Privacy Management (DPM, co-located with ESORICS 2019), September 26-27, 2019, Luxembourg.

1.3 Thesis Organization

The rest of the thesis is organized as follows. In Chapter 2, we first present a brief overview of hotspots and literature review of web tracking, ad injection in web content, and privacy risks of public WiFi hotspots. In Chapter 3, we present our comprehensive analysis for evaluating privacy risks of Canadian public WiFi captive portals, and in Chapter 4, we present our comparative study of privacy practices of public WiFi captive portals in Europe, Canada, and the US. In Chapter 5, we present our evaluation for Canadian public WiFi privacy policies.

Chapter 2

Background and Related Work

This chapter covers some necessary background and literature related to this dissertation.

2.1 Background

Hotspot access is usually deployed in three forms: captive portal, direct/open-access (no captive portals), or password-protected networks. In captive portal networks, users first go through a captive portal session before getting internet access. The captive portal webpage usually displays the privacy policy and/or the terms-of-service (TOS) document, along with some advertisements, and sometimes an option to select the preferred language (for viewing the portal content), and a social login or registration form. After accepting the policy/TOS documents, the user's browser is often directed to a *landing* page, as chosen by the hotspot owner. The captive portal is used to make sure that guests are aware of the hotspot privacy policy, collect personal identification information such as name and email

for future communications, and authenticate guests if needed.

2.2 Related Work

2.2.1 Hotspots Privacy Risks

Several prior studies have demonstrated the possibility of eavesdropping WiFi traffic to identify personal sensitive information in public hotspots. For example, Cheng et al. [13] collected WiFi traffic from 20 airports in four countries, and found that two thirds of the travelers leak private information while using airport hotspots for web browsing and smartphone app usage. Sombatruang et al. [54] conducted a similar study in Japan by setting up 11 experimental open public WiFi networks. The 150-hour experiment confirmed the exposure of private information, including photos, email addresses, confidential documents, and users' credentials—transmitted via HTTP. In contrast, we analyze web tracking and privacy leakage within WiFi captive portals and landing pages. Klasnja et al. [34] studied privacy and security awareness of WiFi users by monitoring web traffic of 11 users. The study shows the users' limited understanding of risks associated with WiFi usage, and a false sense of safety.

2.2.2 Web Tracking

Web tracking, a widespread phenomenon on the internet, is used for varying purposes, including: targeted advertisements, identity checking, website analytics, and personalization. Web tracking techniques can generally be categorized as stateful and stateless.

Stateful tracking [2] is a process where third-party trackers can track users across websites by storing a unique identifier in the user's device. Modern web browsers provide several avenues that can be used to store persistent information. Common techniques include the following:

- HTTP cookies [8] are small files stored on computers. They fall into two categories: persistent cookies and session cookies. While persistent cookies remain on the user device until the cookie is explicitly erased or expired, session cookies are temporary and are erased at the end of the browsing session, upon closing the browser tab.

- Web Storage [43] can be viewed as an improvement to cookies, providing a much greater storage capacity, without any automatic expiry. See also IndexedDB [27].

- Flash cookies [6] are stored on the user device by websites that use Adobe Flash. Note that Adobe will stop supporting Flash at the end of 2020 [4].

Stateless tracking [21] techniques are used to generate a unique device ID based on the combination of a wide range of user device or browser characteristics that might uniquely identify the user device. Several browser APIs including Screen, Navigator, Canvas, or WebGL are used for such device fingerprinting.

Eckersley [19] showed that 83.6% of the Panopticlick website [47] visitors could be uniquely identified from a fingerprint composed of only 8 attributes. User Agent, HTTP ACCEPT headers and if cookies were enabled; the following from JavaScript AJAX posts: screen resolution, time zone, browser plug-ins; and from Java or Flash applet: System fonts.

Laperdrix et al. [36] showed that AmIUnique.org can uniquely identify 89.4% of fingerprints composed of 17 attributes, including the HTML5 canvas element and the WebGL API. In a more recent large-scale study, Gómez-Boix et al. [25] collected over 2 million real-world device fingerprints (composed of 17 attributes) from a top French website; they found that only 33.6% device fingerprints are unique, raising questions on the effectiveness of fingerprinting in the wild. Note that developing advanced fingerprinting techniques to detect the so-called *golden image* (the same software and hardware as often deployed in large enterprises), is an active research area—see e.g., [35, 52]. Several automated frameworks have also been designed for large-scale measurement of web tracking in the wild; see e.g., FPDetective [3] and OpenWPM [21]. In this work, we measure tracking techniques in captive portals and landing pages, and use OpenWPM to verify the prevalence of the found trackers on popular websites.

2.2.3 Detecting Ad Injection

Previous work has also looked into ad injection in web content, see e.g., [49, 57]. We use similar methods for detecting potential similar content injection in hotspots since such incidents have been reported in the past (e.g., [39, 48, 60]).

Previous work has also looked into ad injection in web content. For example, Reis et al. [49] found that some ISPs inject advertisements and unwanted client script in traffic, by comparing the Document Object Model (DOM) sent from a server, with the DOM received by the user. Tsirantonakis et al. [57] showed that some open HTTP proxy servers perform content manipulation and ad injection. They utilize two decoys websites (i.e., honeysites)

designed with different level of complexities to identify any alteration to the honeysites served by the proxies. We use similar methods for detecting potential content injection in hotspots since such incidents have been reported in the past (e.g., [39, 48, 60]).

2.2.4 Analyzing Privacy Policies

A privacy policy usually discloses the service provider's data practices. However, these policies are often long and difficult to read. Several past studies utilize Natural Language Processing (NLP) techniques to analyze privacy policies at scale, e.g., both Sadeh et al. [50] and Harkous et al. [28] use NLP and machine learning techniques to extract important privacy information from policies, and display it to a user in a friendly manner.

Chapter 3

Our Evaluation Framework and Analysis of Canadian Hotspots

In this chapter, we present a comprehensive privacy analysis of 67 unique public WiFi hotspots located in Montreal, Canada, and shed light on the web tracking and data collection behaviors of these hotspots. We design a data collection framework (`CPInspector`)[3] for both Windows and Android, and capture raw traffic traces from several public WiFi hotspots (in Montreal, Canada) that require users to go through a captive portal before allowing internet access. Our study reveals the collection of a significant amount of privacy-sensitive personal data through the use of social login (e.g., Facebook and Google) and registration forms, and many instances of tracking activities, sometimes even before the user accepts the hotspot's privacy and terms of service policies. Most hotspots use persistent third-party tracking cookies within their captive portal site; these cookies can be used

[3] https://github.com/MadibaLab/CPInspector

to follow the user's browsing behavior long after the user leaves the hotspots, e.g., up to 20 years. Additionally, several hotspots explicitly share (sometimes via HTTP) the collected personal and unique device information with many third-party tracking domains.

3.1 CPInspector for Windows

In this section, we describe CPInspector, the platform we develop for measuring captive portal web-tracking and privacy leakages; see Figure 1 for the Windows variant. As Android uses a special app for captive portal, we modify CPInspector accordingly; see Sec. 3.2.

3.1.1 CPInspector Design

The main components of CPInspector include: a browser automation framework, a data migration tool and an analysis module. Selenium is used to visit the hotspot captive portal and perform a wide range of measurements. It collects web traffic, HTTP cookies, WebStorage, fingerprints, browsing profiles, page source code, privacy policy, and screen shots of rendered pages (used to verify the data collection process). CPInspector utilizes Wireshark to capture traffic between the instrumented browser and the hotspot access point. CPInspector uses WebExtensions APIs[4] to collect relevant data (e.g., HTTP cookies, JavaScript calls) from the instrumented browser. Selenium is also used to isolate the test environment from the regular user environment, ensuring that our tests remain unaffected by the user's past browsing behaviors. We also save a copy of the privacy policy, if available. The datasets

[4] https://wiki.mozilla.org/WebExtensions

collected from the hotspots are parsed and committed to a central SQLite database. CPInspector's analysis module then examines the recorded data for tracking behaviors or privacy leaks.

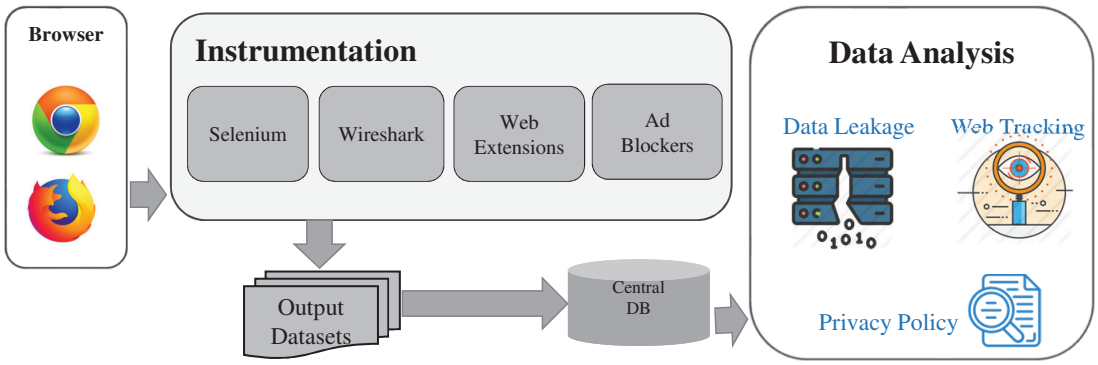


Figure 1: CPInspector design (Windows Setup).

Capturing traffic. We use Wireshark to capture all traffic between the instrumented browser and the hotspot access point. We filter out traffic generated by normal activities such as anti-virus scanning and Windows updates. Moreover, since some captive portals adopt TLS for communication, we rely on the SSLKEYLOGFILE [29] to decrypt the TLS traffic; we then use Tshark [61] to extract and save the HTTP requests/responses to our database.

Identifying third-parties. We identified the corporate websites for each hotspot. Then, we use the WHOIS registration records to identify third-party domains by comparing the domain owner name to the hotspot corporate website owner. All evaluated hotspots have an official website except Hvmans Cafe, where all domains are classified as third-parties. In cases where the domain information is protected by the WHOIS privacy policy, we visit the domain to detect any redirect to a parent site; we then lookup the parent site's

Table 1: Example of variations of the same third-party domain.

Third-Party Request-URL	Blacklisted
https://www.google-analytics.com/r/collect?v=&_v=&a=&t=&_s=1&dl=&ul=&de=&dt=&sd=&sr=&vp=&je=&_u=&jid=&gjid=&cid=&tid=&_gid=&_r=1&gtm=&cd1= &cd64= &cd65= &did= &z=	Yes
https://www.google-analytics.com/j/collect?v=&_v=&a=&t=&_s=&dl=&ul=&de=&dt=&sd=24-bit&sr=&vp=&je=&_u= &jid= &gjid=&cid=&tid=&_gid=&_-r=&cd1=&cd5=&cd6=&cd8=&cd9=&z=	No

registration information. If this fails, we manually review the domain's `Organization` in its TLS certificate, if available. Otherwise, we try to identify the domain owner based on its WHOIS registration email; e.g., addthis.com is owned by Oracle as apparent from its WHOIS email domain-contact_ww_grp@oracle.com. Next, we complement our domain-to-company mapping using the Whotracks.me Trackers List [32]. Finally, we also use Crunchbase [16] and Hoovers [30] to determine if the organizations are subsidiaries or acquisitions of larger companies; e.g., instagram.com is owned by Instagram, which in turn is owned by Facebook.

Identifying third-party trackers. We use EasyList [18], EasyPrivacy, and Fanboy to identify known third-party trackers. EasyList identifies known advertising-related trackers, EasyPrivacy detects known non-advertising-related trackers, and Fanboy's list classifies known social media related trackers. These lists rely on blacklisted script names, URLs, or domains, which may fail to detect new trackers or variations of known trackers. For this reason, we classify third-party trackers as follows: (a) A *known tracker* is a third-party that has already been identified in the above blacklists. (b) A *possible tracker* is any third-party that can potentially track the user's browsing activities but not included in a blacklist. We observed variations of well-known trackers such as Google Analytics, were missed by the

blacklists (see Table 1). Throughout the thesis, we use the word "domain" to refer to the site's fully qualified domain name (FQDN). This definition of domain is commonly used in many studies such as [58, 62].

Ad injection detection. Our framework also includes a module to detect modifications to user traffic, e.g., for ad injections. We visit two decoy websites (i.e., honeysites in our control and hosted on AmazonAWS) and BBC.com, via a home network and a public hotspot, and then compare the differences in the retrieved content (i.e., DOM trees [20]). The use of honeysites allows us to avoid any false positive issues due to the website's dynamic content (e.g., dynamic ads). However, we also include a real website in our experiments (BBC.com). The first honysite is a static web page while the second is comprised of dynamic content that has four fake ads that incorporates JavaScript elements, iframe tags, and four fake ads. The fake ads were created based on source code snippets from Google Adsense, Google TagManager, Taboola.com, and BuySellAds.com. We host the honeysites through Amazon AWS and carefully mimic a realistic website.

3.1.2 Data collection

We collected a total of 679 datasets from the captive portal and landing page of 80 hotspots (12 hotspots are measured at multiple physical locations) between September 2018 to April 2019. We stopped collecting datasets from different locations of the same chain-business as the collected datasets were largely the same. We discarded 103 datasets due to some errors (e.g., network failures). We analyzed over 18.5GB of collected traffic for privacy exposure and tracking measurements, and report the results from 67 unique hotspots (576

Table 2: List of evaluated hotspots From Montreal (Canada).

Category	**Count**	**Hotspot Name**
Cafe and Restaurant	19	A&W, Bombay Mahal Thali, Burger King, Cafe Osmo, Copper Branch, Domino's Pizza, Harvey's, Hvmans Cafe, Juliette Et Chocolat, McDonald's, Moose BAWR, Nespresso, Pizza Hut, Pizza Pizza, Starbucks, Sushi STE-Catherine, The Second Cup, Tim Hortons, Vua Sandwiches
Retail business	17	Canadian Tire, Dynamite, ECCO, Fossil, GAP, Garage, H&M, Home Depot, IGA, Ikea, Laura, Maison Simmons, Michael Kors, Roots, SAQ, Sephora, Walmart
Shopping Mall	12	Atrium 1000, Carrefour Angrignon, Carrefour Laval, Carrefour iA, Centre Eaton, Centre Rockland, Complexe Desjardins, Fairview Pointe-Claire, Mail Champlain, Place Montreal Trust, Place Vertu, Place Ville Marie
Bank	5	CIBC Bank, Desjardins 360, RBC Bank, ScotiaBank, TD Bank
Art and Entertainment	4	Grevin Montreal, YMCA, Montreal Science Centre, Place Des Arts
Transportation	3	Gare d'Autocars de Montreal, Via Rail Station, YUL Airport
Telecom Kiosk	2	Fido, Telus
Car Rental	1	Discount Car Rental
Gymnasium	1	Nautilus Plus
Hospital	1	CHU Sainte-Justine
Hotel	1	Fairmont Hotel
Library	1	Westmount Public Library

datasets). We discuss the results in Sec. 3.1.3.

For the ad injection experiments, we collected a total of 368 datasets from crawling the two honey websites and the BBC.com website at 98 hotspot locations. 11 hotspots are measured at multiple physical locations. We analyzed over 8.7GB of collected traffic for ad injection, and report the results from 87 unique hotspots (368 datasets). We did not observe

any content modification attempts.

3.1.3 Analysis and Results

In this section, we present the results of our analysis on collected personal information, privacy leaks, web trackers, HTTP cookies, and fingerprinting, and the effectiveness of two anti-tracking extensions and private browsing mode.

3.1.3.1 Personal Information Collection, Sharing, and Leaking

Personal identifiable information (PII) collection. Most hotspots (40; 59.7%) allow internet access without seeking any explicit personal data. The remaining 27 (40.3%) hotspots use social login (Facebook, LinkedIn, Google, Instagram) , or a registration page to collect significant amount of personal information; 19 (28.4%) of these hotspots mandate social login or user registration, see Table 3. For instance, the Hvmans Cafe hotspot reads the user's profile information and media from Instagram (See Figure 9 in Appendix B for an example). The profile may include: the user's email address, mobile phone number, user ID, full name, gender, biography, website, and profile picture. Moreover, LinkedIn shares the user's full name, email address, profile picture, LinkedIn headlines, current employment, and basic profile (See Figure 8 in Appendix B for an example). The basic profile consists of a large list of PII items, including full employment history, and the current location [40].

Sharing with third-parties. Most hotspots share personal information and browser/device

[5]In November 2018, we found that Roots was using Yelp WiFi with mandatory personal data collection, but as of April 2019, they now use Cisco that requires no PII.

Table 3: Personal information collected via social login, registration, or optional surveys. The "Powered By" column refers to third-parties that provide hotspot services (when used/identified). F refers to Facebook, L: LinkedIn, I: Instagram, G: Google, T: Twitter, R: registration form, and S: survey; *: personal information is mandatory to access the service.

Hotspot	Powered By	Name	Email	Gender	Birthday	Phone Number	Current City	Profile Picture	Home Town	Country	Facebook Likes	Facebook Friends	LinkedIn Headline	Current Employment	Postal Code	# of Children	Basic Profile	Instagram Media	Tweets	People You Follow
Bombay Mahal Thali*	Sy5	FR	FR		F		F													
Carrefour Laval*	Aislelabs	FR	FR	FR	F		F	F	F		F									
Fairview Pointe-Claire*	Aislelabs	FR	FRT	FR	F		F	F	F		F								T	T
Carrefour Angrignon	Eye-In	FGL	FGL					FGL					L	L			L			
Centre Eaton	Eye-In	F	F					F												
Centre Rockland	Eye-In	FL	FL					FL					L	L			L			
Desjardins 360*	JoGoGo	F	F	F	F	R		F				F								
Domino's Pizza			R																	
Dynamite*			R																	
GAP			R																	
Garage*			R																	
Grevin Montreal	Eye-In	FL	FL				F	FL					L	L	S	S	L			
Harvey's*	Colony Networks	F	FR					F												
Hvmans Cafe*	Purple	FR	FR		F		F	F			F						I	I		
Mail Champlain	Eye-In	FL	FL					FL					L	L			L			
Maison Simmon*			R																	
Michael Kors*	Purple	R	R	R	R	R									R					
Montreal Science Centre*	Telus		R																	
Moose BAWR*	Sticky WiFi		R																	
Nautilus Plus*			R																	
Nespresso*	Orange					R														
Place Montreal Trust			R							R					R					
Roots*[5]	Yelp WiFi	R	R																	
Telus*			R																	
Sushi STE-Catherine*	MyWiFi		R																	
Vua Sandwiches*	Coolblue	FR	FR			R		F												
YUL Airport*	Datavalet	FL	FRL					FL					L	L			L			

information with third-parties via the referrer header, the request-URL, HTTP cookie or WebStorage (for examples, see Table 4 which provides examples from our datasets for these four types of leakage).

We identified 40 hotspots (59.7%) that use third-party captive portals where they share personal information, including 18 (26.9%) share email address; 15 (22.4%) share user's full name; 12 (17.9%) share profile picture; 5 (7.5%) share birthday, current city, current employment and LinkedIn headline; see Table 3. We also found some captive portals leak

Table 4: Examples of MAC address leakage to third-parties via different methods. URL query strings are truncated for brevity.

(1) Leaks via Request URL

```
GET collect?..=HTTP://ca..&client_mac=02:21:5a:4f:d4:49
Host: www.google-analytics.com
```

(2) Leaks by Referer Header

```
GET__utm.gif?utmwv=5.7.2&utms=2&utmn=499018663
Host: www.google-analytics.com
Referer: HTTP:..//?..=HTTP://..&client_mac=02:f6:2e:6c:80:68
```

(3) Leaks by HTTP Cookie

```
Host: msn.com
Cookie: _cb_svref=HTTP://68.67.41.214:8880/... id=02:16:76:70:d4:07
```

(4) Leaks by Web Storage

```
Host: optimizely.com
localstorage: visitor_profile=hReferer:HTTP://../id=02:16:76:70:d4:16
```

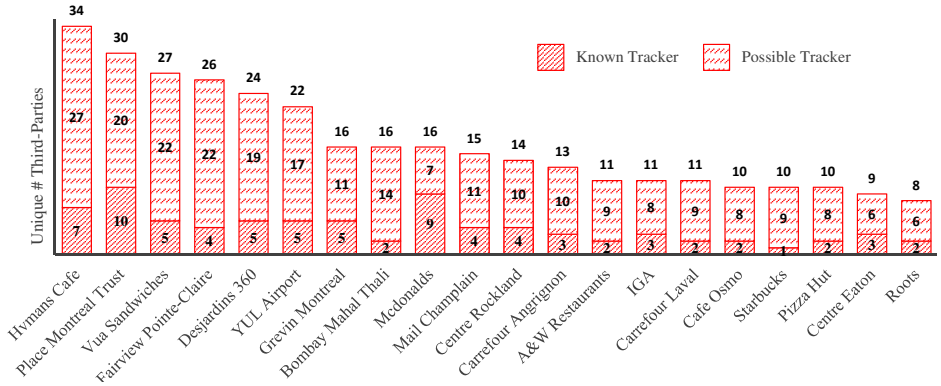
device/browser information to third-parties, including 40 (59.7%) leak MAC address and last visited site; 18 (26.9%) leak screen resolution; 26 (38.8%) leak user agent; 24 (35.8%) leak browser Information and language; and 15 (22.4%) leak plugins. Moreover, some hotspots leak the MAC address to third-parties, e.g., Pizza Hut to 11 domains, and H&M, Place Montreal Trust and Discount Car Rental to six domains each. Top organizations that receive the MAC addresses include: Network-auth.com from 21 hotspots, Alphabet 18, Openh264.org 12, Facebook 10, Datavalet 8, and Amazon 6.

PII leaks via HTTP. We search for personal information of our used accounts in the collected HTTP traffic, and record the leaked information, including the HTTP request URL, and source (captive portal vs. landing page). Three hotspots transmit the user's full name via HTTP (Place Montreal Trust, Nautilus Plus and Roots). In Place Montreal Trust, the user's full name is saved in a cookie (valid for five years), and each time the user connects to the captive portal, the cookie is automatically transmitted via HTTP. Moreover,

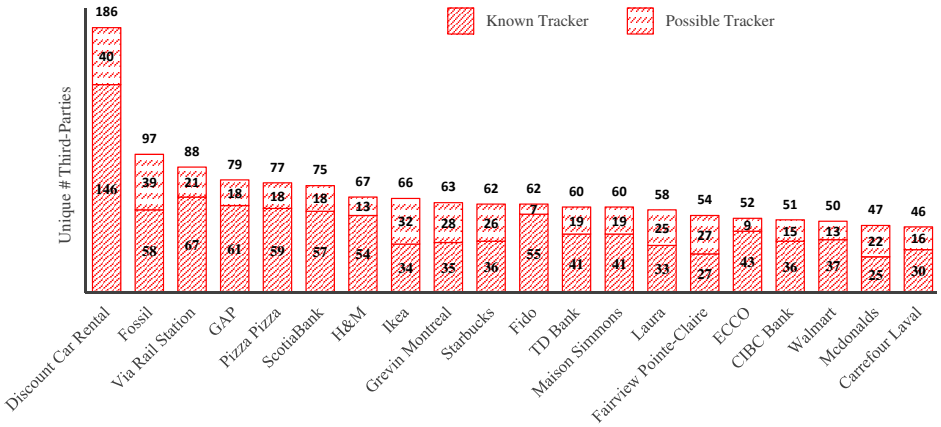
three hotspots leak the user's email address via HTTP (Dynamite, Roots, and Garage). In Nautilus Plus, a user must enter her membership number in the captive portal. For partially entered membership numbers, the captive portal verifies the identity by displaying personal information of five people in a scrambled way (first and last names, postal codes, ages, dates of birth, and phone numbers), over HTTP. The user then chooses the right combination corresponding to her personal information. We also confirmed that some of this data belongs to real people by authenticating to this hotspot using ten randomly generated partial membership numbers. Then, we used the reverse lookup in canada411.ca to confirm the correlation between the returned phone numbers, names, and addresses.

3.1.3.2 Presence of Third-Party Tracking Domains and HTTP Cookies

Tracking domains. We detect third-party tracking domains using: EasyList, EasyPrivacy, and Fanboy's List—downloaded on September 2018. On average, each captive portal hosts 7.4 third-party tracking domains (max: 34 domains, including 10 known trackers); see Figure 3.2(a). We noticed that the hotspots that use the same third-party captive portal still have a different number of third-parties. For example, for the Datavalet hotspots (YUL Airport, McDonald's, Starbucks, Via Rail Station, Tim Hortons, CIBC Bank, Place Vertu), the number of third-parties are 22, 16, 10, 8, 5, 5, and 2 respectively. The hotspots (46; 68.7%) that redirect users to their corporate websites, host more known third-party tracking domains—on average, 30.6 domains per landing page; see Figure 3.2(b). We also analyze the organizations with the highest known-tracker representations. We group domains by the larger parent company that owns these domains. Alphabet, Facebook, and Datavalet



(a) Captive portals



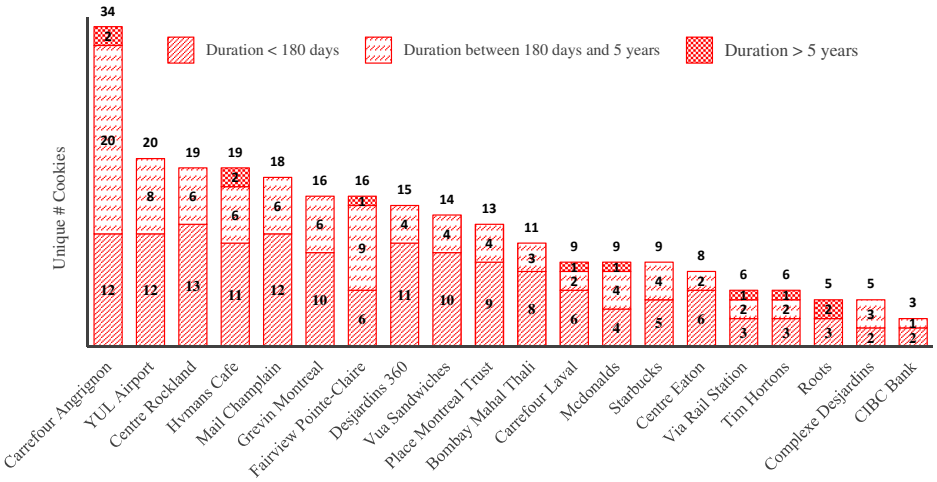
(b) Landing pages

Figure 2: Number of third-party domains on captive portals and landing pages (top 20). For example, Hvmans Cafe captive portal hosts a total of 34 tracking domains, including 7 known trackers. Note that for all reported tracking/domain statistics, we accumulate the distinct tracking domains as observed in all the datasets collected for a given hotspot (e.g., from both browsers and for different social logins, if required). For list of evaluated hotspots see Table 2.

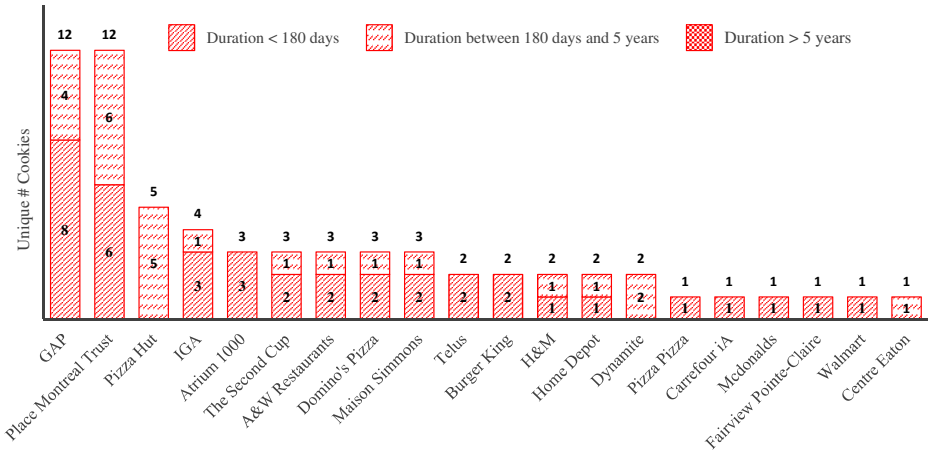
are present on over 10% of the captive portals. Alphabet and Facebook are also present on over 50% of the landing pages.

HTTP tracking cookies on captive portals. We found 40 (59.7%) hotspots create third-party cookies valid for various duration—e.g., over 5 years from 10 (14.9%) hotspots, six months to five years from 23 (34.3%) hotspots, and under six months from 38 (56.7%) hotspots; see Figure 3.3(a). Via Rail Station, Fairview Pointe-Claire, Carrefour Laval, Roots, McDonald's, Tim Hortons, and Harvey's have a third-party cookie from network-auth.com, valid for 20 years. Moreover, YUL Airport, Via Rail Station, Complexe Desjardins, McDonald's, Starbucks, Tim Hortons, CIBC Bank have a common 1-year valid cookie from Datavalet, except for CIBC (17 days). This cookie uniquely identifies a device based on the MAC address (set to the same value unless the MAC address is spoofed). Some hotspots save the MAC address in HTTP cookies, including CHU Sainte-Justine, Moose BAWR, and Centre Rockland. Refer to Table A for the list of cookies that are valid for more than five years.

We also analyze first-party cookies on captive portals; see Figure 3.3(b). 22 (32.8%) hotspots create first-party cookies valid for various durations; 14 (20.9%) hotspots include cookies valid for periods ranging from six months to five years, and 17 (25.4%) hotspots for less than 6 months. Place Montreal Trust saves the user's full name in a first-party cookie valid for five years; this cookie is transmitted via HTTP. Finally, we analyze hotspots that create persistent cookies before explicit consent from the user, we found 26 (38.8%) hotspots create cookies that are valid for periods varying from 30 minutes to a year, including Domino's Pizza, Fido, GAP, H&M, McDonald's, Roots, Starbucks, and Tim Hortons.

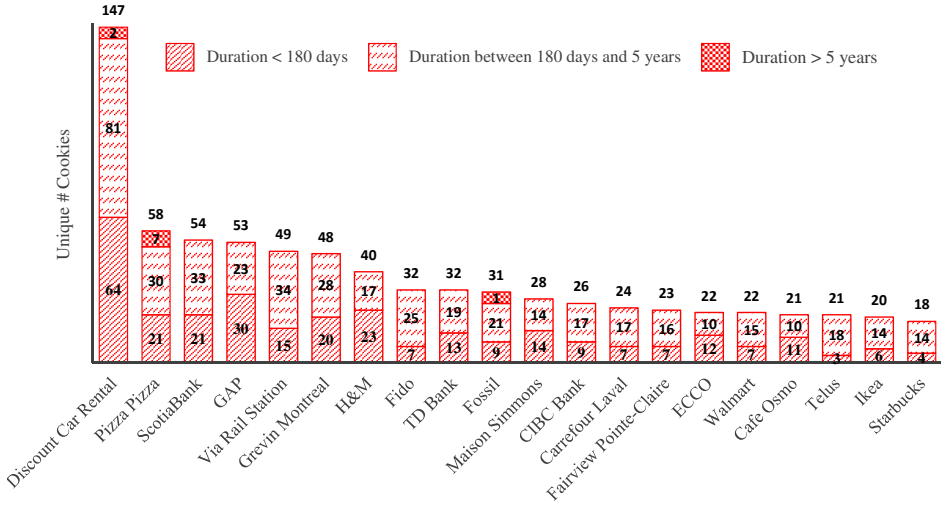


(a) Third-party cookies

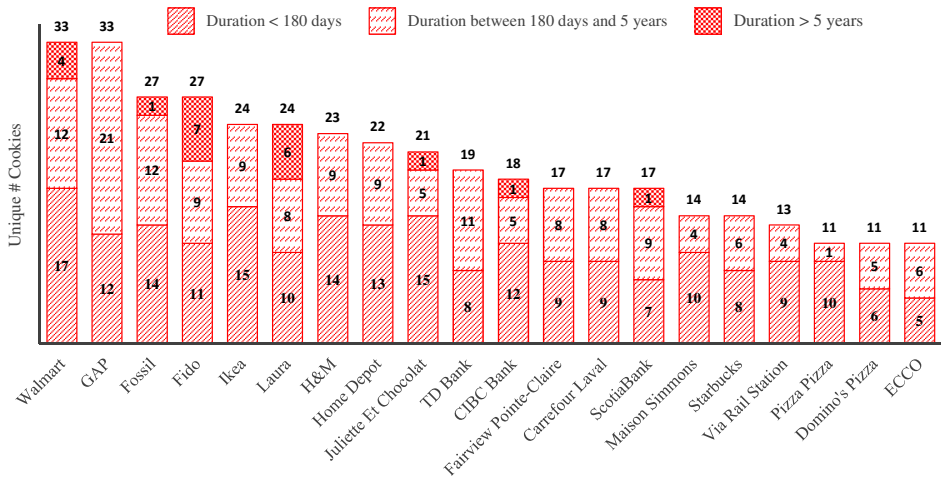


(b) First-party cookies

Figure 3: Number of third-party and first-party cookies on captive portals (top 20). Note that for all reported cookies/domain statistics, we accumulate the distinct cookies as observed in all the datasets collected for a given hotspot. We consider a cookie as a potential tracking cookie if the cookie is persistent (i.e., session cookies are ignored).



(a) Third-party cookies



(b) First-party cookies

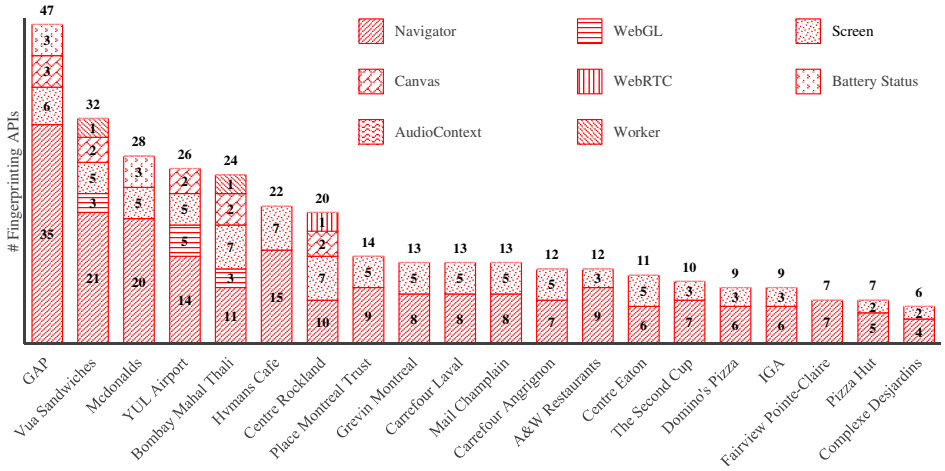
Figure 4: Number of third-party and first-party cookies on landing pages (top 20). Note that for all reported cookies/domain statistics, we accumulate the distinct cookies as observed in all the datasets collected for a given hotspot. We consider a cookie as a potential tracking cookie if the cookie is persistent (i.e., session cookies are ignored).

HTTP tracking cookies on landing pages. We found 48 (71.6%) hotspots create third-party cookies valid for various durations—e.g., over 5 years from 4 (6.0%) hotspots, six months to five years from 47 (70.1%) hotspots, and under six months from 42 (62.7%) hotspots, see Figure 3.4(a). Prominent examples include the following. Fossil has a 25-year valid cookie from pbbl.com; CIBC Bank has two 5-year valid cookies from stackadapt.com, a known tracker. We also analyze the first-party cookies on landing pages; see Figure 3.4(b). 42 (62.7%) hotspots create first-party cookies valid for various durations—e.g., over 5 years from 10 (14.9%) hotspots, six months to five years from 42 (62.7%) hotspots, and under six months from 41 (61.2%) hotspots. Notable examples: Fossil has a 99-year valid cookie, Fido has three cookies valid for 68–81 years, CHU Sainte-Justine has a 20-year valid cookie, CIBC Bank has a 19-year cookie, and Walmart has four cookies valid for 9–20 years.

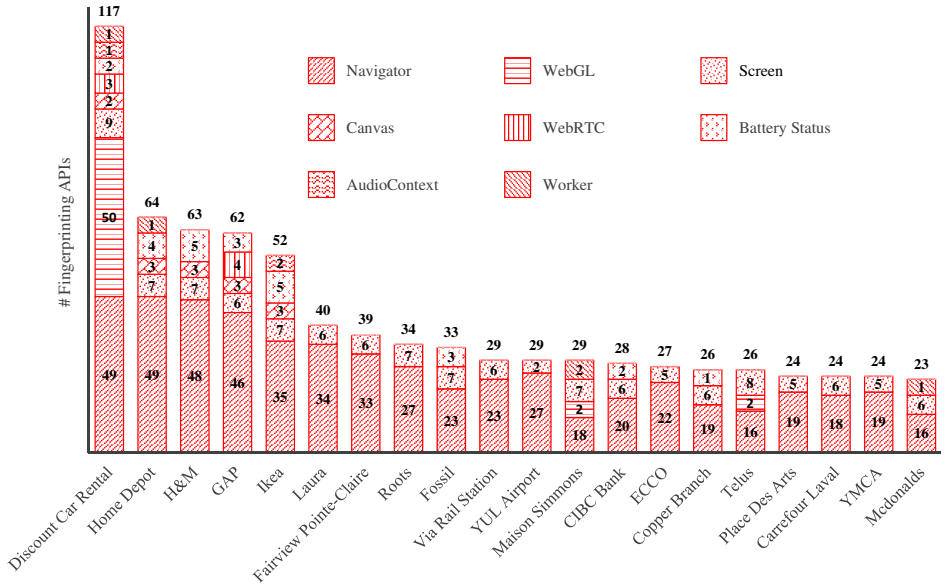
3.1.3.3 Device and Browser Fingerprinting

We analyze fingerprinting attempts in captive portals and landing pages. We use Don't FingerPrint Me (DFPM [33]) for detecting known fingerprinting techniques, including the screen object, navigator object, WebRTC, Font, WebGL, Canvas, AudioContext, and Battery Status [21, 41, 44, 46]. We use attribute and API interchangeably, when referring to fingerprinting JavaScript APIs.

Captive portal. 24 (35.8%) hotspots perform some form of fingerprinting. On average, each captive portal uses 5.9 attributes (max: 47 attributes, including 35 Navigator, 6 Screen, 3 Canvas, and 3 Battery Status); see Figure 3.5(a). We also found 10 (14.9%) hotspots



(a) Captive portals



(b) Landing pages

Figure 5: Number of fingerprinting APIs on captive portals and landing pages (top 20). Note that for all fingerprinting statistics, we accumulate the distinct APIs as observed in all the datasets collected for a given hotspot.

fingerprint user device/browser before explicit consent from the user, including GAP, McDonald's, and Place Montreal Trust, using 6–46 attributes. Moreover, 46 (68.7%) hotspots fingerprint MAC addresses.

Landing pages. 51 (76.1%) hotspots perform fingerprinting on their landing pages. On average, each landing page fingerprints 19.4 attributes (max: 117 attributes, including 49 Navigator, 9 Screen, 2 Canvas, 3 WebRTC, 50 WebGL, 1 AudioContext, 1 Worker and 2 Battery Status); see Figure 3.5(b). Prominent examples include the following. Discount Car Rental includes script from Sizmek Technologies Inc., which uses a total of 67 APIs (48 WebGL, 12 Navigator, five Screen, and two Canvas APIs). Manual analysis also reveals Font fingerprinting via side-channel inference [44]; this script is also highly similar to FingerprintJS [59]. Discount Car Rental also uses script from Integral Ad Science, which uses 41 attributes, including: 31 Navigator, seven Screen APIs, two WebRTC, and one AudioContext (cf. [21]). The navigator APIs are used to collect attributes such as the USB gamepad controllers, and list MIDI input and output devices. H&M and Home Depot host the same JavaScript that collects 42 attributes, including 34 Navigator, six Screen, and two Canvas APIs. Laura has a script from PerimeterX that collects 27 attributes, including 21 Navigator and 6 Screen APIs; code manual analysis reveals WebGL and Canvas fingerprinting.

3.2 CPInspector for Android

In contrast to Windows, Android OS handles captive portals with a dedicated application. The Android Developers documentation and Android Source documentation omit details of how Android handles captive portals. Here we briefly document the inner working of Android captive portals, and discuss our preliminary findings, specifically on tracking cookies on Android devices.

3.2.1 Android Captive Portal Login App

Using Android `ps` (Process Status), we observe that a new process named `com.android.captiveportallogin` appears whenever the captive portal is launched. The Manifest file for CaptivePortalLogin explicitly defines that its activity class will receive all captive portal broadcasts by any application installed on the OS and handle the captive portal. We observe that files in the data folder of this application are populated and altered during a captive portal session; we collect these files from our tests.

3.2.2 Capturing Network Traffic

To capture traffic from Android apps, several readily-available VPN apps from Google Play can be used (e.g., Packet Capture, NetCapture, NetKeeper). However, Android does not use VPN for captive portals. On the other hand, using an MITM Proxy server such as mitm-proxy (https://mitmproxy.org/) requires the server to run on a desktop environment, which would make the internet traffic come out of the desktop OS, i.e., the mobile device would

not be visible to the hotspot. To overcome this, we set up a virtual Linux environment within the Android OS by using Linux Deploy (https://github.com/meefik/linuxdeploy), enabling us to run Linux desktop applications within Android with access to the core component of Android OS, e.g., Android OS processes, network interfaces, etc. We use Debian and mitmproxy on the virtual environment, and configure Android's network settings to proxy all the traffic going through the WiFi adapter to the mitmproxy server. The proxy provides us the shared session keys established with a destination server, enabling us to decrypt HTTPS traffic. We use tcpdump to capture the network traffic.

3.2.3 Data Collection and Analysis

We visited 22 hotspots and collect network traffic from their captive portals. First, we clear the data and cache of the CaptivePortalLogin app and collect data from a given hotspot. Next, we change the MAC address of our test devices (Google Pixel 3 with Android 9 and Nexus 4 with Android 5.1.1) and collect data again without clearing the data and cache. From the proxy's request packets, we confirm that the browser agent correctly reflects our test devices, and the traffic is being originated from the CaptivePortalLogin app. Next, we analyze the data extracted from the app. The structure of the data directory is similar to Google Chrome on Android. We locate the `.\app_webview\Cookies` SQLite file in the data directory, storing the CaptivePortalLogin app's cookies.

We observe that 9 out of 22 hotspots store persistent cookies in the captive portal app; see Figure 6. These cookies are not erased when the portal app is closed, or when the user

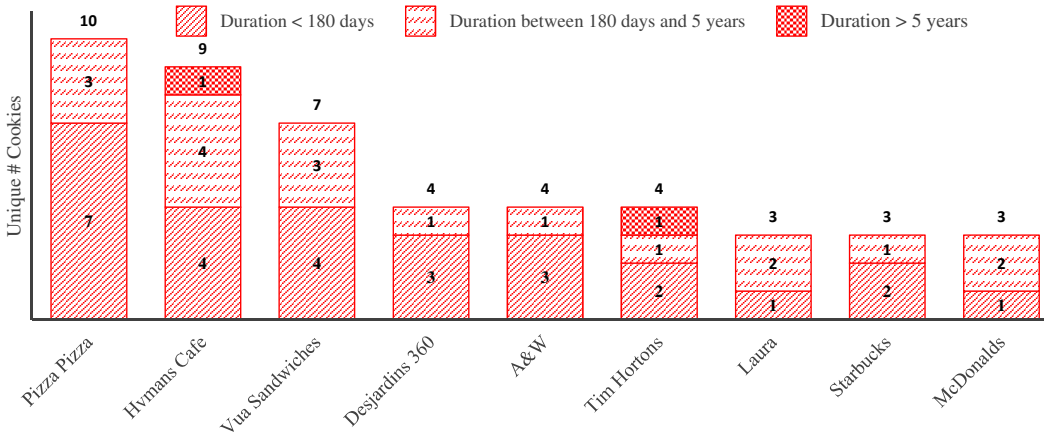


Figure 6: Number of cookies stored on the Android captive portal app. We consider a cookie as a potential tracking cookie if the cookie is persistent (i.e., session cookies are ignored).

leaves the hotspot. Instead, the cookies remain active as set in their validity periods, although they are unavailable to the regular browser apps. Prominent examples include: Tim Hortons inserts a 20-year valid cookie from network-auth.com, and Hvmans Cafe stores a 10-year valid cookie from Instagram. In the captive portal traffic, we confirm that these cookies are indeed present and shared in subsequent visits, and follow the Same-Origin Policy. Hotspots can use these cookies to uniquely identify and authenticate user devices even when the device MAC address is dynamically changed; Tim Hortons hotspot uses its cookies for authentication. However, McDonald's did not authenticate the device even though the cookies were present but the MAC address was new.

3.3 Privacy Policy and Anti-Tracking

3.3.1 Privacy Policy

We performed a preliminary manual analysis of privacy policy and TOS documents from hotspots that appear to be most risky. Roots states clearly in their privacy policy that they use SSL to protect PII, but their captive portal transmits a user's full name and email address via HTTP. Place Montreal Trust transmits the user's full name via HTTP, and they explicitly state that transmission of information over the public networks cannot be guaranteed to be 100% secure. Nautilus Plus has a very basic TOS that omits important information such as the laws they comply with and privacy implications of using their hotspot. They state clearly that the assurance of confidentiality of the user's information is of great concern to Nautilus Plus, but they use HTTP for all communications, leaking personal information while they attempt to verify the customer's identity; see Sec. 3.1.3.1. Their privacy policy is also inaccessible from the captive portal and omits any reference to WiFi. Dynamite and Garage are two brands of Groupe Dynamite. They transmit the user's email address via HTTP despite claiming to use SSL. Their privacy policy is inaccessible from the captive portal and omits any reference to the WiFi. GAP explicitly mentions their collection of browser/device information, and they indeed collect 46 such attributes, *before* the user accepts the hotspot's policies.

Although McDonald's tracks users in their captive portal (9 known trackers, 28 fingerprinting attributes), the captive portal itself lacks a privacy policy stating their use of web tracking. Carrefour Laval and Fairview Pointe-Claire perform cross device tracking

by participating in the Device Co-op [5], where they may collect and share information about devices linked to the user. Two hotspots link the user's MAC address to the collected personal information, including Roots, and Bombay Mahal Thali. Sharing the harvested personal data with subsidiaries and third-party affiliates is also the norm. We found 34 (50.7%) hotspots have a TOS document but lack a privacy policy on their captive portal, including TD Bank, and Burger King. Three hotspots lack both the privacy policy and TOS document on their captive portals, including Laura, ECCO, and Maison Simmons.

3.3.2 The Same Hotspot Captive Portal in Different Physical Locations

12 hotspots are measured at multiple physical locations. We stopped collecting datasets from different locations of the same chain-business as the collected datasets were largely the same. We provide an example where some minor differences occur: Starbucks' captive portal domain varies in the two evaluated locations (am.datavalet.io vs. sbux-j2.datavalet.io). However, the number of known trackers remained the same, while the number of third-parties increased by one domain. Moreover, the `-sf-device` cookie validity increased from 17 days to 1 year, and the `-sf-landing` cookie was not created in the second location.

3.3.3 Effectiveness of Privacy Extensions and Private Browsing

To evaluate the effectiveness anti-tracking solutions against hotspot trackers, we collect traffic from both Chrome and Firefox in private browsing modes, and by enabling Adblock Plus, and Privacy Badger extensions—leading to a total of six datasets for each hotspot. Then, we use the EasyList, EasyPrivacy, and Fanboy's lists to determine whether known trackers remain in the collected datasets; see Table 5. We only count the domain name of a tracker or advertiser when a request was sent, or a cookie was created.

Table 5: The number of unique known trackers not blocked by our anti-tracking solutions.

	W/O Ad Blockers	**AdBlock Plus**	**Privacy Badger**	**Private Browsing**
Firefox	382	33	180	315
Chrome	488	117	212	356

3.3.4 Hotspot Trackers in the Wild

We measured the prevalence of trackers found in captive portals and landing pages, in popular websites—to understand the reach and consequences of hotspot trackers. We use OpenWPM [21] between February 28–March 15, 2019 to automatically browse the home pages of the top 143k Tranco domains [37] as of February 27, 2019. We extract the tracking persistent cookie domains from captive portals or landing pages; we define such cookies to have validity $\geq$ 1 day and the sum of the value lengths from all the cookies from the same third-party website longer than 35 characters—cf. [11]. Then, we counted those tracking domains in the OpenWPM database; see Table 6. For example, the doubleclick.net cookie as found in 4 captive portals and 30 landing pages, appears 160,508 times in the top 143k

Tranco domains (mutiple times in some domains). Overall, hotspot users can be tracked across websites, even long time after the user has left a hotspot.

Table 6: Count of tracking domains from captive portals and landing pages in Tranco domains 143k home pages (top 10).

Captive Portal	
Tracker	**Count**
doubleclick.net	160508
linkedin.com	48726
facebook.com	37107
twitter.com	14874
google.com	13676
atdmt.com	5198
instagram.com	3466
gap.com	295
maxmind.com	294
gapcanada.ca	64

Landing Page	
Tracker	**Count**
pubmatic.com	326991
rubiconproject.com	257643
doubleclick.net	160508
casalemedia.com	131626
adsrvr.org	116438
addthis.com	83221
demdex.net	83160
contextweb.com	82965
rlcdn.com	75295
livechatinc.com	69919

3.4 Summary of Results

We collected a total of 679 datasets from the captive portals and landing pages of 80 hotspot locations between September 2018 to April 2019. 103 datasets were discarded due to some errors (e.g., network failure). We analyzed over 18.5GB of collected traffic for privacy exposure and tracking, and report the results from 67 unique hotspots (576 datasets), making this the largest such study to characterize hotspots in terms of their privacy risks. Our hotspots include cafes and restaurants, shopping malls, retail businesses, banks, and transportation companies (bus, train and airport), some of which are local to Montreal, but many are national and international brands. 40 hotspots (59.7%) use third-party captive

portals that appear to have many other business customers across Canada and elsewhere. Thus, our results might be applicable to a larger geographical scope. We discuss the main findings of our privacy analysis of public WiFi captive portals along five axis:

Data collection. 27 hotspots (40.3%) use social login or a registration page to collect personal information (19 hotspots make this process mandatory for internet access). Social login providers may share several privacy-sensitive PII items—e.g., we found that LinkedIn shares the user's full name, email address, profile picture, full employment history, and the current location.

User tracking. Except three, all hotspots employ varying levels of user tracking technologies on their captive portals and landing pages. On average, we found 7.4 third-party tracking domains per captive portal (max: 34 domains). We also found that 40 hotspots (59.7%) create persistent third-party tracking HTTP cookies (validity up to 20 years); 4.2 cookies on average on each captive portal (max: 34 cookies). Surprisingly, 26 hotspots (38.8%) create persistent cookies even *before* getting user consent on their privacy/TOS document. Furthermore, two hotspots (3.0%) state in their privacy policies that they explicitly link the user's MAC address to the collected PII, allowing long-term user tracking, especially for desktop OSes with fixed MAC. Note that sharing the harvested data with subsidiaries and third-party affiliates is the norm.

From our Android experiments, we reveal that 9 out of 22 hotspots can effectively track Android devices even though Android uses a separate captive portal app and randomizes MAC address as visible to the hotspot.

Data sharing and privacy leaks. Several hotspots explicitly share (sometimes even without HTTPS) personal and unique device information with many third-party domains. 40 hotspots (59.7%) expose the user's device MAC address; five hotspots leak PII via HTTP, including the user's full name, email address, phone number, address, postal code, date of birth, and age (despite some of them claiming to use TLS for communicating such information). Two hotspots appear to perform cross-device tracking via Adobe Marketing Cloud Co-op [5].

Ad/content injection. We also design a framework to detect ad/content injection by hotspots. We collected over 8.7GB traffic (346 datasets) by crawling two honey websites and BBC.com from 98 hotspots (hotspots without captive portals are also included). We did not observe any content modification attempts.

3.5 Conclusion

Public WiFi hotspots are growing in popularity across the globe. Most users frequently connect to hotspots due to their free-of-cost service. This motivates companies to use advertising and tracking services on their public WiFi captive portals and landing pages to understand customers interests, behaviors, and in some cases monetize those hotspots. In this chapter, we perform a comprehensive analysis of web tracking and data collection behaviors of public WiFi hotspots in Montreal, Canada. Our analysis reveals that the majority of hotspots employ varying levels of user tracking technologies on their captive portals and

landing pages. We identify noticeable data collection through the use of social login (e.g., Facebook and Google) and registration forms. We also demonstrate that several hotspots explicitly share (sometimes via HTTP) the collected personal and unique device information with many third-party tracking domains. In fact, more than half of hotspots use third-party captive portals that appear to have many other business customers across Canada and elsewhere. Thus our results might be applicable to a larger geographical scope.

Chapter 4

Analysis of Worldwide Hotspots

In Chapter 3, we analyzed tracking behaviors and privacy leakage in WiFi captive portals and landing pages of 80 hotspot locations (in Quebec, Canada) between September 2018 to April 2019. We reveal the collection of a significant amount of privacy-sensitive personal data through the use of social login (e.g., Facebook and Google) and registration forms, and many instances of tracking activities, sometimes even before the user accepts the hotspot's privacy and terms of service policies. In this chapter, we collected a total of 130 datasets from the captive portal and landing page of 112 hotspots locations in Ontario (39; Canada), Luxembourg (43; Europe), Netherlands (3; Europe), France (2; Europe), and New York (25, USA) between July 2019 to October 2019. Our main objective is to perform a high-level comparison of privacy practices between Canadian, European, and the US hotspots. Our analysis reveals that most hotspots use varying levels of third-party trackers on public WiFi captive portals in the three regions. We also found that more than half of hotspots use third-party captive portals result in sharing the harvested data with third-party entities.

4.1 Methodology

Our main objective here is to perform a high-level comparison of privacy practices between Canadian, European, and the US hotspots, including the use of third-party trackers, and sharing harvested data with third-party entities through the use of third-party captive portals. Our methodology remains mostly the same as Chapter 3. We benefit from the lessons learned from our study on Canadian hotspots. We streamline some of the cases of data collection that did not produce significant results. From each hotspot, we collect traffic using Chrome on Windows. We stop collecting datasets from Firefox as the datasets we collected previously (Chapter 3) were largely the same. We also stop collecting datasets in private browsing, ad-blockers, and Android as the focus in this phase is to compare tracking behaviors between hotspots in Europe, Canada, and the US. In order to perform an apple-to-apple comparison, we only include the previously collected data using the Chrome browser in regular browsing mode from Quebec, Canada in this chapter.

4.2 Data Collection

We conduct two phases of data collections from public WiFi hotspots. In Chapter 3, we collected a total of 679 datasets from the captive portal and landing page of 80 hotspot locations in Quebec, Canada between September 2018 to April 2019. We analyzed the collected traffic for privacy exposure and tracking, and report the results from 67 unique hotspots. In this chapter, we collected a total of 130 datasets from the captive portal and landing page of 112 hotspots locations in Ontario (39; Canada), Luxembourg (43; Europe),

Netherlands (3; Europe), France (2; Europe), and New York (25, USA) between July 2019 to October 2019.[6] In total, we tested the captive portal and landing page of 80 hotspot locations between September 2018 to October 2019 from Europe, Canada, and the US. For summary of the total number of evaluated hotspots in each region, see Table 7. The complete list of evaluated hotspots (including Quebec) is available in Appendix C.

Table 7: List (count) of evaluated hotspots in Europe, Canada, and the US.

Region	# Locations	# Unique hotspots	# Locations per sub region
Canada	119	100	Ontario (39) and Quebec (80)
Europe	48	47	Luxembourg (43), France (2), and Netherlands (3)
US	25	25	New York (25)

4.3 Analysis and Results

4.3.1 Finding the Captive Portal Operator

Our objective is to understand companies involved in the hotspots tracking and data collection in public WiFi hotspots. First, we identified each hotspot captive portal URL. Then, we use the WHOIS registration records to identify the domain owner name. In cases where the domain information is protected by the WHOIS privacy policy, we visit the domain to detect any redirect to a parent site; we then lookup the parent site's registration information. If this fails, we manually review the domain's Organization in its TLS certificate, if

[6]From each hotspot, we collect traffic using Chrome on Windows. We stopped collecting datasets from Firefox as the collected datasets were largely the same. We also stopped collecting datasets in private browsing, ad-blockers, and Android as the focus in this phase is to compare tracking behaviors between hotspots in Europe, Canada, and the US.

available. Otherwise, we try to identify the domain owner based on its WHOIS registration email; e.g., globalsuite.net is owned by Guest-Tek as apparent from its WHOIS email production@guest-tek.com. If the captive portal's owner cannot be identified, we use the captive portal URL's "public suffix + 1" [42] as the company owner. We found the operators for five hotspots (Andersons, Brochettes et Cie, Bombay Mahal Thali, Subway and Ernster) from the "Powered by" message that appear on their captive portal as TP-Link, WiiZone, Sy5, AirTight Networks and MixVOIP, respectively. Finally, we also use Crunchbase [16] to determine if the organizations are subsidiaries or acquisitions of larger companies; e.g., carrols.com is owned by Carrols Corporation, which in turn is owned by Bridgepoint (the parent company of Burger King Corporation). The combination of these methods helped us to accurately find 71 companies owning the captive portal of 141 hotspots. We could not find company information for 46.3% (31 hotspots) of the public WiFi hotspot captive portals in our dataset. Throughout the chapter we use the word "Operator" to refer to the captive portal owner.

4.3.2 Third-Party Captive Portals

Table 8 compares the number of hotspots that use a third-party captive portal in our dataset. As depicted in the table, third-party captive portals are commonly used in many Canadian, European, and the US hotspots. Around 64% of Canadian/European hotspots and 56% of the US hotspots use a third-party captive portal. In total, we identified 108 hotspots (62.8%) that use third-party captive portals in our dataset of the three regions.

Table 8: Analysis of organizations that owns the captive portals in our evaluated hotspots.

	Canadian Hotspots (C)	**European Hotspots (E)**	**The US Hotspots (U)**	$\lvert C \cap E \rvert$	$\lvert C \cap U \rvert$	$\lvert E \cap U \rvert$	$\lvert C \cap E \cap U \rvert$
# Unique hotspots	100	47	25	4	4	1	1
# Hotspots operators	52	34	20	3	5	1	1
# Hotspots w 3rd-party captive portals	64	30	14	-	-	-	-
% Hotspots w 3rd-party captive portals	64.0%	63.8%	56.0%	-	-	-	-

4.3.3 Hotspots Operators

Table 9: List of captive portal operators grouped by their parent company (top 15).

Company	**# hotspots**	**Region**	**Hotspots [max. 3]**
Cisco	24	CA, US, EU	M&T Bank, NBC bank, YMCA
Datavalet	12	CA	McDonald's, Tim Hortons, Starbucks
H&M	7	CA, EU	H&M, Arket, COS
Eye-In	5	CA	Centre Eaton, Grevin Montreal, Mail Champlain
Aislelabs	4	CA	Carrefour Laval, Rideau Centre, South St. Burger
Cloudflare	4	CA, US	Atrium 1000, Place Ville Marie, Maid of the Mist
Cloudi-Fi	4	EU	CHANEL, Cloche d'Or, Gucci
Purple	4	CA	Hvmans Cafe, Walmart, Michael Kors
Bridgepoint	3	CA, US	Burger King(CA), Burger King(US), Tim Hortons (US)
TELUS	3	EU	Telus(Quebec), Telus(Ontario), Montreal Science Centre
Hotspot System	3	EU	KIKI, Rock Box, Zulu
AT&T	2	CA, US	Home Depot, McDonald's
Facebook	2	US, CA	Tinder Box, NYX
Dynamite	2	CA	Dynamite, Garage
GAP	2	CA	GAP(Quebec), GAP(Ontario)

Table 9 shows the top 20 organizations that operate hotspot captive portals. Cisco delivers 14.0% (24) of hotspot services for the three regions. If we look at each region, we find that Cisco operates 2 (4.3%), 17 (17.0%) and 5 (20.0%) hotspots in Europe, and Canada and the

US, respectively. For instance, Cisco operates Bayshore (Canada), Barnes & Noble (US), and MAC cosmetics (Europe).

4.3.4 Operators of Common Hotspots

Table 10: List of common hotspots in the three regions showing the operator in each region.

Hotspot	**Canada**	**Europe**	**US**
Burger King	Bridgepoint	Win	Bridgepoint
McDonald's	Datavalet		AT&T
H&M	H&M Clothing Company	H&M Clothing Company	
Starbucks	Datavalet		GlobalReach Technology
Tim Hortons	Datavalet		Bridgepoint
Pizza Hut	pizzahut.ca	172.16.28.1	
ONroute	HMSHost		
MAC Cosmetics	Cisco	Cisco	

Table 11: List of common hotspots in Quebec and Ontario showing the operators.

Hotspot	Quebec	Ontario
A&W Restaurants	Yum! Brands	Yum! Brands
Fido	Cisco	Cisco
GAP	Gap, Inc.	Gap, Inc.
H&M	H&M Clothing Company	H&M Clothing Company
Laura	Cisco	Cisco
McDonald's	Datavalet	Datavalet
Roots	Yelp WiFi[7], Cisco	Cisco
Sephora	Sephora	Sephora
Starbucks	Datavalet	Datavalet
TD Bank	Toronto Dominion Bank Group	Toronto Dominion Bank Group
Telus	TELUS Corporation	TELUS Corporation
The Second Cup	The Second Cup	The Second Cup
Tim Hortons	Datavalet	Datavalet
Walmart	Purple	Purple

[7]In November 2018, we found that Roots was using Yelp WiFi, but as of April 2019, they now use Cisco in both Ontario and Quebec hotspots.

In Table 10, we analyze the captive portal operator of public WiFi hotspots that have branches in multiple regions. We notice that hotspots sometimes use the same captive portal operator in their different branches. For example, MAC cosmetics uses a captive portal owned by Cisco in their Canadian and European hotspots. We can also see that Burger King uses captive portal from Bridgepoint in the US and Canada while Win (win.be) provides the service in Europe. In contrast, McDonald's, Starbucks, and Tim Hortons are common hotspots between Canada and the US. However, Datavalet owns the three hotspots' captive portals in Canada. In the US, AT&T owns McDonald's captive portal; GlobalReach Technology owns Starbucks captive portal; and Bridgepoint owns the Tim Hortons captive portal. Moreover, in Table 11, we analyze the Canadian hotspots that have branches in different regions in Canada (Quebec and Ontario). Our analysis reveals that all the 14 hotspots have the same operators in their Quebec and in Ontario branches.

4.3.5 Presence of Third-Party Tracking Domains on Captive Portals

In this section, we conduct a high-level comparison of first and third-party domains present on captive portals of Canadian hotspots with those present on captive portals of European and the US hotspots, see Table 12. This comparative analysis uncovers differences in the third-party domains that appear in the three regions. In aggregated terms, we found 45 unique known trackers (FQDNs) in our set of Canadian hotspots but only 21 and 18 in the European and the US hotspots, respectively. However, when looking specifically at the percentage of known trackers, we see that they are slightly more diverse in the US hotspots (32.14%) but only 22.72% and 18.75% in the Canadian and European hotspots,

respectively. The intersection between the unique third-party domains (FQDNs) is also low. Only 12 common third-party domains are presents on the captive portal in the three regions. However, our analysis reveals that on average, each captive portal hosts 5.37, 4.34, and 3.84 third-party tracking domains in Canada, Europe and the US, respectively. The statistics of known trackers reflect only a lower estimate of the presence of third-party trackers on captive portals because of the limitations of EasyList and EasyPrivacy blacklists in detecting new trackers or variations of known trackers [1, 51, 53].

Table 12: Analysis of third-party domains on captive portals of evaluated hotspots.

	Canadian Hotspots (C)	**European Hotspots (E)**	**The US Hotspots (U)**	$C \cap E$	$C \cap U$	$E \cap U$	$C \cap E \cap U$
# Unique hotspots	96[8]	47	25	4	4	1	1
# Unique domains	312	152	91	32	25	12	12
# Unique first-parties	114	40	35	2	2	0	0
# Unique third-parties	198	112	56	30	23	12	12
# Unique known trackers	45	21	18	7	11	3	3
% Unique known trackers	22.72	18.75	32.14	-	-	-	-
Avg third-party trackers	5.4	4.34	3.84	-	-	-	-
Avg known trackers	1.1	0.72	0.8	-	-	-	-

[8] In order to perform an apple-to-apple comparison, we only include the previously collected data using the Chrome browser in regular browsing mode from Quebec, Canada in this study. This reduces the total number of evaluated unique Canadian hotspots in this chapter from 100 to 96 due to technical errors collecting Chrome datasets for four hotpots in Quebec, including CHU Sainte-Justine, Sushi STE-Catherine, The Second Cup, and Westmount Public Library.

We also analyze the first-party in the captive portals. In our analysis, we found no common first-party domains among the three regions. However, two domains are common between Canada and Europe (splashpage.hm.com and hm.com) which represent the captive portal and landing page domains of the H&M hotspots in the two regions. We also found two domains that are common between Canada and the US (McDonalds.com and timhortons.com) which appear on the landing pages of McDonald's and Tim Hortons hotspots, respectively.

Note that for all reported unique domains/first-parties/third-parties/known trackers in Table 12, we accumulate the distinct domains/first-parties/third-parties/known trackers as observed in all the datasets collected for a given region.

4.4 Conclusion

In this chapter, we analyze the privacy of Public WiFi captive portals from different regions: Canada, Europe, and the US. We reveal the use of varying level of third-party trackers on their public WiFi captive portals. We also found the use of third-party captive portal is the norm which results in sharing the harvested data with third-party entities. We also found that some companies operate in the three regions which allows user tracking across countries/continents. This pose some unique risks due to the hotspot access to the users' foot traffic, browsing habits, the device MAC address, and in certain cases, personal information.

Chapter 5

Analysis of Canadian Hotspots' Privacy Policies

In Chapter 3, we analyzed tracking behaviors and privacy leakage in WiFi captive portals and landing pages of 80 hotspot locations (in Montreal, Canada) between September 2018 to April 2019. In this chapter, we analyze hotspots privacy policies and terms-of-use documentation which also discloses the service provider's data and privacy practices. We use our collected hotspots' datasets to validate some of those privacy practices, including data collection, secure data transfer, data storage location, and data sharing. The results presented in Chapter 3 reveal the collection of a significant amount of privacy-sensitive personal data through the use of social login (e.g., Facebook and Google) and registration forms. Several hotspots explicitly share (sometimes via HTTP) the collected personal and unique device information with many third-party tracking domains. In this chapter, we evaluated a sample of 16 privacy policy and TOS documents from hotspots that appear

to be most risky in Montreal, Canada; Table 13 summarizes the results of our analysis. Briefly, in this chapter, we propose a group of criteria to analyze various privacy aspects in hotspots and we use our collected hotspots' datasets to validate selected privacy aspects of the public WiFi.

5.1 Privacy Policy Evaluation Framework

In this section, we outline a group of criteria that are representative of various privacy aspects in hotspots. The criteria we explore consist of five categories: privacy policies and terms-of-service documentation, data collection, third-party sharing, data security, and web tracking. This set of criteria is initially inspired by Mahmoud et al. [38] and Harkous et al. [28], and then interactively refined throughout our study. For every criterion, a hotspot may fully or partially satisfy it, not satisfy it, or may not provide relevant information.

Privacy policy and TOS documentation. An easily accessible privacy policy/TOS is important for communicating any privacy implications to the hotspot users.

P1 Captive-portal-links: The captive portal contains a link to the privacy policy document.

P2 Policy-change-information: The privacy policy has an update date; and the hotspot notifies users of any changes to its privacy policy.

P3 TOS-Captive-portal-links: The captive portal contains a link to the TOS document.

P4 TOS-change-information: The TOS document has an update date; and the hotspot notifies users of any changes to its terms of service.

Data collection. Hotspots may collect a wide range of personal information from users

while trying to get access to the internet. We define the following criteria to evaluate data collection practices in public WiFi hotspots:

C1 Laws-compliant-stated: The hotspot defines clearly the laws they comply with in its privacy policy, and the jurisdiction(s) in which they operate.

C2 Report-data-collection: The hotspot is transparent about its data collection practices. We validate the company actual data collection practices noted during our evaluation of each hotspot.

C3 Collection-purpose-stated: The hotspot clearly communicates reasons for collecting user information.

C4 No-children-data-collection: The hotspot must have a clear policy about data collected from children and provide the ability for parents to permanently delete the collected information.

C5 No-data-MAC-address-link: The hotspot does not link the MAC address to any personal information.

C6 PII-access-edit-delete: Users can access, edit or permanently delete the information collected by the hotspot; partially granted if any option is missing.

Third-party sharing. Hotspots may share users' data with third-parties and affiliates. We define the following criteria to highlight hotspot's user data sharing practices with third-parties.

D1 No-third-party-data-sharing: The hotspot must explicitly state in its privacy policy that it does not share any personal information. We inspect all communications between the captive portal and back-end servers for third-party data sharing. We also check if the

hotspots use third-party captive portals where they share personal information with third-party.

D2 No-data-selling: The hotspot must explicitly state in its privacy policy that it does not sell any personal information.

Data security. Protecting users' information is a major concern as any leak could lead to identification of individual users and their location. We define four features under this category.

S1 Data-storage-location: The location of data storage is stated in privacy policy and it matches the actual server location in our collected datasets.

S2 Secure-data-transfer: The measures taken by the hotspot captive portal operator to protect the collected information is properly documented in the privacy policy. We verify this criteria by inspecting the hotspot use of TLS for all communications between the captive portal and back-end servers.

S3 Dedicated-privacy-support: The hotspot has a dedicated support for privacy related issues and concerns.

S4 Unsecure-internet-stated: The TOS must clearly state if the hotspot does not provide any level of encryption to protect user data from eavesdropping (such as WEP, WPA or other encryption mechanisms).

Web tracking. Hotspots can use various techniques to track users. This includes identifiers locally stored on the user's device by third-parties (e.g., HTTP cookies), which are commonly used to uniquely identify users. We define the following criteria to highlight data web tracking practices in hotspots.

U1 No-cookies-before-user-consent: The captive portal should not perform any web tracking activities before the user consents her acceptance of terms and conditions. Currently, we simply rate a hotspot by inspecting all communications between the captive portal and back-end servers.

U2 Do-not-track-support: The documentation clearly states how the captive portal handles Do Not Track (DNT) requests. DNT is an option available in some browsers, designed to allow users to opt-out of web tracking.

Table 13: Comparative evaluation of selected hotspots' privacy policies.

Hotspot	***P1 Captive-portal-links***	***P2 Policy-change-information***	***P3 TOS captive-portal-links***	***P4 TOS-change-information***	***C1 Laws-compliant***	***C2 Report-data-collection***	***C3 Collection-purpose-stated***	***C4 No-children-data-collection***	***C5 No-data-MAC-address-link***	***C6 PII-access-edit-delete***	***D1 No-third-party-data-sharing***	***D2 No-data-selling***	***S1 Data-storage-location***	***S2 Secure-data-transfer***	***S3 Dedicated-privacy-support***	***S4 Unsecure-internet-stated***	***U1 No-cookies-before-user-consent***	***U2 Do-not-track-support***
Bombay Mahal Thali	◑	○	●	○	●	●	○		○		○		○	○	○	●	●	
CF Carrefour Laval	●	◑	●	○	●	○	●		◑	◑	○	●	○	●	●	●	●	
CF Fairview Pointe Claire	●	◑	●	○	●	○	●		◑	◑	○	●	○	●	●	●	○	
Carrefour Angrignon	◑	○	●	○	●	○	●			◑	○	●	○	○	○	●	●	
Centre Eaton	●	●	●	○	●	●	●	●		◑	○		○	●	●	●	●	
Centre Rockland	◑	◑	●	○	●	○	●	●		◑	○		○	●	●	●	○	○
Domino's Pizza	●	◑	●	○	●	●	●	●	◑	◑	○		○	●	●	●	○	
Dynamite*	○	◑	●	○	●	●	●	●			○	●	○	○	●	●	●	
Garage*	○	◑	●	○	●	●	●	●			○	●	○	○	●	●	○	
Grevin Montreal	◑	○	●	○	●	○	●		◑	◑	○	●	○	○	○	●	●	
Hvmans Cafe	●	○	●	○	●	○	●		◑	●	○		●	●	●	●	●	
Mail Champlain	◑	◑	●	○	●	○	●	●	◑	◑	○		○	●	●	●	●	○
Nautilus Plus*	○	○	●	○		●	●	●	◑		●	●	○	○	○	○	●	
Place Montreal Trust	●	●	●	○	●	●	●	●	◑	◑	○	●	○	○	●	●	○	
Roots	●	○	●	○	●	●	●	●	○	◑	○		○	○	●	●	○	
Vua Sandwiches	◑	◑	●	◑	●	○	●		◑	◑	○		○	●	○	○	●	

●= offers the options; ◑= partially offers the option; ○= does not offer the option; no circle = info. is unavailable.
(*) = There is no link to the document from the captive portal.

5.2 Overview of Results

In this section, we present our evaluation for a sample of 16 representative policies of hotspots that collect personal information from users; see Table 18 in Appendix D for links to the documents.

For each hotspot, we manually inspect the privacy policy and TOS documents that appear on the hotspot captive portal between September 2018 to April 2019. For three hotspots, the captive portal did not have a link to the privacy policy document, hence we evaluated the company privacy policy published on their website, including Dynamite, Garage, and Nautilus Plus. A hotspot may appear to conform to privacy best practices according to its documentation, but may fail to implement necessary technical measures. Therefore, we use our collected hotspots' datasets to validate some privacy practices, including secure data transfer, data storage location, and data sharing. We emphasize that our evaluation here is based on available privacy policies, terms of use documents and analyzing web traffic collected while testing each public WiFi. We discuss the findings of our review of hotspots privacy policies along five axes; for a quick summary of our results refer to Table 13. Section 5.3 explains the evaluation results for each hotspot.

Privacy policy and TOS documentation. We first look at whether the privacy policy and TOS can be found easily on the public WiFi captive poral, and if users are notified upon privacy policy and TOS changes. We found that 7 out of 16 hotspots provide a direct link to their policies in their WiFi captive portal, 6 hotspots have the TOS and privacy policy documents merged into one document, and 3 hotspots do not provide a direct link to their

policies in their WiFi captive portal. However, although the changes to the privacy policy and TOS are hard to be regularly monitored by public WiFi users, only 4 out 16 of public WiFi hotpots stated that they actively notify users upon policy changes (Dynamite, Garage, centre Eaton, Place Montreal Trust), and one public WiFi hotspot (Domino's Pizza) posts a notice of TOS changes to the captive portal.

Data collection. We first study the data collection behavior in the hotspots. We found the data collection is mandatory to access the service in half of hotspots. We also found half of hotspots fail to report what kind of data is collected from users to access the service. Moreover, we found 15/16 hotspots define generic reasons for collecting data from public WiFi users, such as marketing and advertisement, customer survey, and for protecting users and property. COPPA [24] states a verifiable parental consent must be obtained before gathering any data from children below 13 years old. However, only 9/16 hotspots stated that their service is not to be used by the children under the age of thirteen and provided the possibility for the parent to delete their children data if it was collected without parental consent. We found 11/16 hotspots read the user MAC address, but only two hotspots stated explicitly that they link PII to MAC address—allowing long-term user tracking, including Roots, and Bombay Mahal Thali. Finally, we found 11/16 allow users to access or edit their information. However, seven hotspots do not state if the user can request to delete the personal information, including Domino's Pizza, Grevin Montreal, and Vua Sandwiches. Moreover, three hotspots stated that it may be impossible to completely delete user information without some residual information (e.g., due to backup), including Centre Eaton, Roots, and Carrefour Angrignon. Alternatively, Hvmans Cafe states that customers can

access/edit/delete their data by contacting the data protection officer. Lastly, we found that most privacy policies (15/16) states explicitly the laws/acts they comply with. All 15 hotspots except Hvmans Cafe, comply with laws and courts of Canada while Hvmans Cafe complies with laws and courts of Wales (U.K.). However, Nautilus Plus omits any information about laws and courts from its privacy policy.

Third-party sharing. We first investigate personal data sharing with third-party. In total, we found 15/16 hotspots that share personal and unique information. For instance, we found 11/16 hotspots that use third-party captive portals where they share personal information with third-party, including Roots, and Bombay Mahal Thali; see Table 3 in Chapter 3. By inspecting our collected network traffic, we also found 2/16 hotspots share the user's MAC address with third-party domains, including Domino's Pizza and Place Montreal Trust; both hotspots do not use a third-party captive portal. Moreover, we also found 2/16 hotspots stated that they may share personal information with internal and external service providers, including Dynamite and Garage. However, we could not find any network traffic in our dataset that in practice match the company stated data sharing policy. In contrast, Nautilus Plus states that they may share data with third-party if required by law. Finally, we found half of hotspots explicitly stated that they do not sell customer personal information, including Nautilus Plus.

Data security. We first study the data storage location; we found 8/16 hotspots (including Hvmans Cafe, Fairview Pointe-Claire, and Carrefour Laval) stated that PII may be stored outside Canada. However, the Hvmans Cafe is the only public WiFi among the eight hotspots that clearly states the data storage location is New York (which match the actual

server location in our datasets [9]). We also found half of hotspots omit any information about the PII storage location, including Dynamite and Vua Sandwiches. Next, we study whether the public WiFi hotspot takes the necessary measures (e.g., makes use of encryption) to transfer personal information to the server. Primarily, we check the policies to see if the hotspot states which security measures are used to protect personal information. We found 12/16 hotspots discuss security measures in their privacy policies. However, 7/12 of those hotspots concluded that no collection or transmission of information over the Internet can be guaranteed to be 100% secure, including Centre Rockland, Place Montreal Trust, and Roots. After that, we verify the hotspots network traffic of those hotspots and we found 4/12 hotspots do not conform with their privacy policies since they send personal information via HTTP. Two hotspots transmit the user's full name via HTTP (Place Montreal Trust and Roots). In Place Montreal Trust, the user's full name is saved in a cookie (valid for five years), and each time the user connects to the captive portal, the cookie is automatically transmitted via HTTP. Moreover, three hotspots leak the user's email address via HTTP (Dynamite, Roots, and Garage). So in total, we found 8/16 hotspots comply with secure-data-transfer (S2) criteria.

Web tracking. The European General Data Protection Regulation(GDPR) [45] have clear provisions stating that websites must display a (cookie) consent notice prior to saving cookies on the user browser. However, we found 6/16 hotspots create persistent cookies even *before* getting user consent on their privacy/TOS documents. We also study if the hotspot

[9]We find the server location by extracting the contacted IP address of the hotspot main domain from network traces then use the Reverse IP Address lookup API(http://free.ipwhois.io/json/) to identify the server location information

clarifies the danger of using un-encrypted public WiFi in their TOS; and we found 14/16 comply with this criterion. We also found two hotspots explicitly stated that they do not respond to the browser "Do not track" signals.

5.3 Detailed Evaluation of Privacy Policies

In this section, we present individual evaluation for the hotspots reviewed in this chapter where we elaborate on how we rate each hotspot.

5.3.1 Bombay Mahal Thali Hotspot

Bombay Mahal Thali hotspot is powered by SY5 [55]. It partially satisfies Captive-portal-links; it includes some privacy information in the TOS document, including collection of personal information (e.g., Facebook information). Nevertheless, it does not satisfy Update-info-information (P2 and P4) because it does not state the last date of update in the documentation, and at the same time, it states that the users must check back the TOS for any changes, implying that the hotspot does not notify the user with changes. The hotspot states that it collects user's email address, date of birth, and current city. It also states that they may collect PII from (i) Facebook basic information, including age, birthdate, name, gender; extended profile information, including events, check-ins, Facebook likes, interests, friends, friends of friends, groups. (ii) Twitter profile, including screen name, name, location, profile picture. The user cannot use the service without providing an email address or sign-in using a Facebook account. In practice, they collect less information

than stated (name, email address, birthday, and current city), hence, we rate this hotspot as satisfying Report-data-collection (C2) feature. This hotspot does not satisfy no-data-MAC-address-link (C5) criteria because it links PII to MAC address as stated explicitly in the privacy policy. The hotspot lacks data-storage-location (S1); its captive portal domain in the US as appears from collected network traffic. The hotspot does not satisfy the secure-data-transfer (S2) as the hotspot does not explain security measures implemented to protect user personal information. It also does not use HTTPS protocol for all web traffic which expose the MAC address and last visited site. It also does not satisfy Dedicated-privacy-support (S3) as they have a generic email address for sharing privacy concerns. The hotspot lacks no-third-party-data-sharing (D2) because the hotspot shares data with third-party captive portal. Finally, the hotspot is governed by the federal laws of the province of Ontario and the federal laws of Canada.

5.3.2 CF Fairview Pointe Claire and CF Carrefour Laval hotspots

CF Fairview Pointe Claire and CF Carrefour Laval are two shopping malls that are managed by Cadillac Fairview [12]. The two hotspots are powered by Aislelabs [7] and have the same TOS and privacy policy documents. Both hotspots partially satisfy update-info-information (P2) since they fail to notify the user with any update details to the privacy policy, although the policy indicates the update date. They also do not satisfy update-info-information (P4) as they do not include the last update date in the TOS, and they may update the TOS without notifying the users. The user cannot use the service without providing an email address or sign-in using a Facebook account. In practice, the hotspots collect the

name, email address, gender, birthday, current city, profile picture, hometown, and Facebook likes using social media accounts and registration form. However, the privacy policy does not clarify exactly what information is collected from social accounts. Hence, we rate the two hotspots as not satisfying Report-data-collection (2) feature. They also stated that they collect information through social media when the user post information related to the company, its service or its properties. They also mention that they collect usage information, such as pages viewed or searched for; and that they collect browser and device information, such as browser type and version, operating system, MAC address, and device type. Both hotspots stated that PII are stored in Canada. However, they may use service providers who process or store information outside of Canada. The two hotspots partially satisfy no-data-MAC-address-link (C5) because they read the user device MAC address so, they may link PII to the MAC address. Finally, the hotspot is governed by the laws and courts Canada.

5.3.3 Carrefour Angrignon

Although Carrefour Angrignon is powered by Eye-In [22] but the privacy policy document is slightly different from the Mail Champlain and Centre Rockland hotspots, powered by the same company. Carrefour Angrignon has the TOS and privacy policy documents merged into one document. Hence captive-portal-links (P1) is rated as partially provided. It does not satisfy update-info-information (P2) as it does not include the last update date in the privacy policy section, and at the same time, it does not notify the user

with changes (similar rating for TOS P4). The hotspot collects name, email address, profile picture, LinkedIn headlines, current employment, Tweets, and people you follow from LinkedIn. However, the privacy policy only states that they collect MAC addresses and/or IP addresses, hence, we rate the hotspot as lacking support to report-data-collection (C2) feature. Carrefour Angrignon states that personal information about user will not be sold without the user's approval. We rate Carrefour Angrignon as partially satisfying PII-access-edit-delete (C6) because although it allows users to access/update/delete PII but the policy states that it may be impossible to completely delete user information without some remaining residue. The hotspot lacks data-storage-location (S1); its captive portal domain in the US. It also does not satisfy dedicated-privacy-support (S3) as the user can share privacy concerns through a generic email address or by sending a regular mail to the company. We rate the hotspot as satisfying the collection-purpose-stated (C3) since it states that the company uses the collected data for operation and security; fraud prevention; and protecting users and property. The hotspot lacks no-third-party-data-sharing (D2) because the hotspot shares data with third-party captive portal. Finally, the hotspot is governed by the laws and courts of Quebec (Canada).

5.3.4 Centre Eaton

Although Centre Eaton is powered by Eye-In [22], the privacy policy document is completely different from the other hotspots powered by the same company. However, Centre Eaton shares the same policy and TOS with Place Montreal Trust as they are both owned by Ivanhoe Cambridge [31]. Centre Eaton does not satisfy update-info-information (P4)

as it does not include the last update date in the TOS, and it may update the TOS without notice to users. Centre Eaton satisfies update-info-information (P2) as it includes the last update date in the privacy policy, and it notify users of the existence of a new Privacy Policy. The privacy policy provides a clear description of the personal information that might be collected. In practice, the hotspot collects the name, email address, and profile picture. Hence, we rate the hotspot as supporting the report-data-collection (C2) feature. We rate Centre Eaton as partially satisfying PII-access-edit-delete (C6) because although it allows users to request to access/update/delete PII but the policy clarifies it may be impossible to completely delete customer information without some residual information because of backups. The hotspot does not satisfy data-storage-location (S1); the hotspot may store users' personal information outside of Canada. We rate the hotspot as satisfying the collection-purpose-stated (C3) since it states that the company uses the collected data for example, to understand and assess customers interests. Centre Eaton states that personal information about user will not be sold without the user's approval. The hotspot lacks no-third-party-data-sharing (D2) because the hotspot shares data with third-party captive portal. Finally, this hotspot is governed by the laws and courts of Quebec (Canada).

5.3.5 Centre Rockland and Mail Champlain

Centre Rockland and Mail Champlain are two shopping malls that are managed by Cominar [14]. The two hotspots are powered by Eye-In [22]. They share the same TOS and privacy policy documents. Both documents are merged together. Hence captive-portal-links (P1) is rated as partially provided. They also partially satisfy update-info-information

(P2) as they include the last update date in the privacy policy section; and at the same time, they stated that the users must check back the document for any changes, implying that the hotspot does not notify the user with changes. They do not satisfy update-info-information (P4) as they do not include the last update date in the TOS section, and they fail to mention whether they keep the users updated with any changes in the TOS section. The hotspot collects name, email address, profile picture, LinkedIn headlines, current employment, and LinkedIn basic profile. However, the privacy policy only states that they collect personal information but did not specify exactly which information they are collecting from the user's account, hence, we rate the hotspot as lacking support to report-data-collection (C2) feature. We rate both hotspots as partially satisfying PII-access-edit-delete (C6) because although they allow users to inspect PII by contacting the privacy manager, the policy does not state if the user can request to update/delete the personal information. Although both hotspots have the same policy; they are hosted on two different domains. This affects the no-cookies-before-user-consent (U1) evaluation as Centre Rockland creates two cookies valid for 30 minutes before user consent while Mail Champlain does not. Moreover, Centre Rockland has a cookie that has the user's device MAC address while Mail Champlain does not have this cookie, which imply completely different implementation of the hotspots' captive portals. They do not satisfy data-storage-location (S1) as they may store the information in Canada or the US or any other country. We rate the hotspot as satisfying the collection-purpose-stated (C3) since it states that the company uses the collected data for example, to send information about services, promotions, surveys. The hotspot lacks no-third-party-data-sharing (D2) because the hotspot shares data with third-party captive

portal. Finally, the two hotspots are governed by the laws and courts of Quebec (Canada).

5.3.6 Domino's Pizza Hotspot

Domino's Pizza hotspot partially satisfies update-info-information (P2) because it does not contain the last date of update in the privacy policy, although, they stated that a notice is posted for privacy policy changes on its homepage. Moreover, it does not state how users are notified of any TOS changes, and at the same time, it does not contain the last date of update in the TOS, thus not fulfilling update-info-information (P4). The privacy policy provides a clear description of the personal information that might be collected (name, email address and telephone). In practice, the hotspot collects the email address. Hence, we rate the hotspot as supporting the report-data-collection (C2) feature. We rate Domino's Pizza as partially satisfying PII-access-edit-delete (C6) because although it allows users to access/update PII by contacting the privacy manager, the policy does not state if the user can request to delete the personal information. It does not satisfy no-third-party-data-sharing (D2) since it shares personal information with professional advisors, suppliers, franchisees, agencies, and provides users' personal information in case of a law or court order. The hotspot also shares the user's MAC address with network-auth.com. We rate Domino's Pizza as not satisfying the no-cookies-before-user-consent (U1) as it creates a cookie from the domain network-auth.com, which is valid for 31 days before the user clicks the Connect button. We rate the hotspot as satisfying the collection-purpose-stated (C3) since it states that the company uses the collected data for example, to receive deals. The hotspot lacks data-storage-location (S1); its captive portal domain in the US. This hotspot

partially satisfies no-data-MAC-address-link (C5) because they read the user device MAC address so, they may link PII to the MAC address. Finally, this hotspot governed by the laws and courts of Ontario (Canada).

5.3.7 Dynamite and Garage Hotspots

Dynamite and Garage are two brands of Groupe Dynamite. They use the same terms of service for their hotspots. Both hotspots do not provide privacy policy documents, hence captive-portal-links (P1) and update-info-information (P2) features are inapplicable. However, we evaluated their privacy policy documents that are available on their website. Both hotspots do not include the last update date in the privacy policy, and their privacy policies stated that they may notify users about important changes by email or other means. They do not satisfy update-info-information (P4) as they do not include the last update date in the TOS, and do not notify users with updates in the TOS. The user cannot use the service without providing an email address. However, the privacy policy states that email address may be collected for the user to receive email updates. Hence, we rate this hotspot as satisfying report-data-collection (C2) feature. Although the two hotspots stated that they provide the necessary measures to protect personal information, they leak the user's email address via HTTP. Hence, they do not satisfy the secure-data-transfer (S2). We rate the hotspot as satisfying the collection-purpose-stated (C3) since it states that the company uses the collected data for example, to receive offers. They do not sell personal information, except if its part of the sale of all or part of the company business or a property. The hotspots do not satisfy no-third-party-data-sharing (D2) criterion because the hotspots

stated in their policy that they may share personal information with internal and external service providers but we did not find any traces for sharing data with third-parties in the web traffic. The hotspots lack data-storage-location (S1); their captive portal domains in the Canada. This hotspot partially satisfies no-data-MAC-address-link (C5) because they read the user device MAC address so, they may link PII to the MAC address. Finally, the two hotspots are Laws-compliant with the laws of the province where the service is used.

5.3.8 Grevin Montreal Hotspot

Although Grevin Montreal is powered by Eye-In [22], its document is slightly different from most hotspots powered by the same company, including Mail Champlain, Centre Rockland, and Carrefour Angrignon hotspots. Grevin Montreal has the TOS and privacy policy documents merged into one document. Hence, captive-portal-links (P1) is rated as partially provided. It does not satisfy update-info-information (P2) as it does not include the last update date in the privacy policy section; and at the same time, it does not notify the user with changes (similar rating for TOS P4). Grevin Montreal states that personal information about user will not be sold without the user's approval. The hotspot collects name, email address, current city, profile picture, LinkedIn headlines, current employment, # of kids, and postal code, and LinkedIn basic profile. However, the privacy policy only states that they collect MAC addresses and/or IP addresses, hence, we rate the hotspot as lacking support to report-data-collection (C2) feature. We rate Grevin Montreal as partially satisfying PII-access-edit-delete (C6) because although it allows users to access/update PII, the policy does not state if the user can request to delete the personal information. The

hotspot does not satisfy the secure-data-transfer (S2) as the hotspot does not explain security measures implemented to protect user personal information. It also does not use HTTPS protocol for all web traffic which expose the device's MAC Address. It does not satisfy dedicated-privacy-support (S3) since it has a generic email address and specifies possibility to send a regular mail to generic address for sharing privacy concerns. The hotspot lacks data-storage-location (S1); its captive portal domain in the US. We rate the hotspot as satisfying the collection-purpose-stated (C3) since it states that the company uses the collected data for example, marketing purposes. The hotspot lacks no-third-party-data-sharing (D2) because the hotspot shares data with third-party captive portal. Finally, this hotspot is governed by the laws and courts of Quebec (Canada).

5.3.9 Hvmans Cafe Hotspot

Hvmans Cafe Hotspot does not satisfy update-info-information (P2) feature since it does not include the last update date in the policy, and does not notify users with policy updates (similar rating for TOS P4). The hotspot collects user's full name, email address, current city, profile picture, Facebook likes, Instagram profile information and media. The Instagram profile includes the user's email address, mobile phone number, user ID, full name, gender, biography, website, and profile picture. However, the privacy policy only states that they name, postal address, phone number, email address, date of birth, gender, and social media account details (such as Facebook, Twitter, Instagram, etc.) without much details on information that are shared from social media account, hence, we rate the hotspot as

lacking support to report-data-collection (C2) feature. The hotspot satisfies data-storage-location (S1); it stores the user's personal Information in New York for data collected in North and South America. We rate the hotspot as satisfying the collection-purpose-stated (C3) since it states that the company uses the collected data for example, to communicate with customers or to offer customers relevant goods and services. The hotspot lacks no-third-party-data-sharing (D2) because the hotspot shares data with third-party captive portal. We rate Hvmans Cafe as satisfying PII-access-edit-delete (C6) because it allows users to access/update/delete PII upon providing a proof of their identity. Finally, this hotspot governed by the laws and courts of Wales (U.K.).

5.3.10 Nautilus Plus Hotspot

Nautilus Plus hotspot does not provide a link to the privacy policy document, hence the captive-portal-links (P1), and policy-change-information (P2), features are inapplicable. However, we evaluated its privacy policy document that is available on their website. This privacy policy does not include the last update date in the privacy policy, and it does not state that they may notify users about important changes. The hotspots lack data-storage-location (S1); its captive portal domain could not be located due to the use of local IP address. The user cannot use the service without providing an email address. However, the privacy policy states that email address may be collected for the user to receive newsletter and promotions. Hence, we rate this hotspot as satisfying report-data-collection (C2) feature. This hotspot partially satisfies no-data-MAC-address-link (C5) because they read the user device MAC address so, they may link PII to the MAC address. The hotspot does

not satisfy the secure-data-transfer (S2) as the hotspot does not explain security measures implemented to protect user personal information. It also does not use HTTPS protocol for all web traffic which leak the user's personal information. The leak happens while the user tries to connect to the hotspot. In Nautilus Plus, a user must enter her membership number in the captive portal. For partially entered membership numbers, the captive portal verifies the identity by displaying personal information of five people in a scrambled way (first and last names, postal codes, ages, dates of birth, and phone numbers), over HTTP. The user then chooses the right combination corresponding to her personal information. We also confirmed that some of this data belongs to real people by authenticating to this hotspot using ten randomly generated partial membership numbers. Then, we use the reversed lookup in canada411.ca to confirm the correlation between the returned phone numbers, names, and addresses.

5.3.11 Place Montreal Trust Hotspot

Although Place Montreal Trust is powered by Eye-In [22], its documents are completely different from most hotspots powered by the same company. However, Place Montreal Trust shares the same policy and TOS with Center Eaton as they both owned by Ivanhoe Cambridge [31]. Place Montreal Trust does not satisfy update-info-information (P4) since it does not include the last update date in the TOS, and it may update the TOS without notice to users. Place Montreal Trust satisfies update-info-information (P2) since it includes the last update date in the privacy policy, and it notify users of the existence of a new Privacy Policy. The privacy policy provides a clear description of the personal information

that might be collected. In practice, the hotspot collects the name, country, and postal code. Hence, we rate the hotspot as supporting the report-data-collection (C2) feature. We rate Place Montreal Trust as partially satisfying PII-access-edit-delete (C6) because although it allows users to access/update PII but the policy does not specify clearly if the user can request to delete the personal information. However, the hotspot may store users' personal information outside of Canada. Although the hotspots states that they provide the necessary measures to protect personal information, they leak the user's full name via HTTP. Hence, they do not satisfy the secure-data-transfer (S2). We rate Place Montreal Trust as not satisfying the no-cookies-before-user-consent (U1) since it creates multiple cookies before the user clicks the Connect button. These persistent cookies are valid for periods varying from several days to a year. We rate the hotspot as satisfying the collection-purpose-stated (C3) since it states that the company uses the collected data for example, to understand and assess customers interests. The hotspot shares the user's MAC address with third-party domains, including network-auth.com and doubleclick.net. Finally, this hotspot is governed by the laws and courts of Quebec (Canada).

5.3.12 Roots Hotspot

Roots hotspot uses third-party captive portal powered by Yelp WiFi [63] for its hotspot. In this hotspot, the users must enter their full name, and email to be granted access to the internet; and their MAC address and PII are linked together as clearly stated in the policy. Yelp WiFi states that they work with the Future of Privacy Forum [23] to ensure their

practices adhere to the most ethical and moral standards. It does not provide the update-info-information (P2) because it does not state the last date of update and it states that users must check back the policy for any changes, implying that they do not notify the user with changes. It does not satisfy update-info-information (P4) because it does not state the last date of update and it states that users must check back the TOS for any changes, implying that they do not notify the user with changes. The privacy policy provides a clear description of the personal information that might be collected (e.g., name, email address and telephone). In practice, the hotspot collects the email address. Hence, we rate the hotspot as supporting the report-data-collection (C2) feature. The hotspot is governed by the laws and courts of Ontario and the federal laws of Canada. We rate roots hotspot as partially satisfying PII-access-edit-delete (C6) because although they allow users to access/update PII but the data cannot be completely deleted due to their backup process. Although the hotspots states that they provide the necessary measures to protect personal information, they leak the user's full name via HTTP. Hence, they do not satisfy the secure-data-transfer (S2). It is also leaked if an adversary capture and reply the HTTP traffic, and in this case the user's full name appears in the browser to the attacker, see Figure 7. We rate the Roots' hotspot as not satisfying the no-cookies-before-user-consent (U1) since it creates a cookie from the domain network-auth.com, which is valid for 31 days before the user clicks the Connect button. This hotspot also does not satisfy no-data-MAC-address-link (C5) because they explicitly stated that they link PII to MAC address. The hotspot lacks data-storage-location (S1); its captive portal domain in the US. We rate the hotspot as satisfying the collection-purpose-stated (C3) since it states that the company uses the collected data for

example, to improve marketing and promotional efforts. The hotspot lacks no-third-party-data-sharing (D2) because the hotspot shares data with third-party captive portal. Finally, the hotspot is governed by the federal laws of the province of Ontario and the federal laws of Canada.

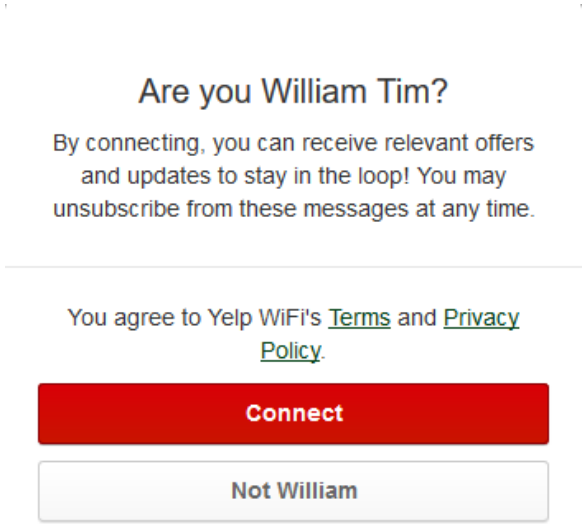


Figure 7: Roots hotspot leaks the user full name if an adversary capture and reply the HTTP traffic, and in this case the user's full name appears in the browser to the attacker.

5.3.13 Vua Sandwiches Hotspot

Vua Sandwiches is powered by coolblue [15]. Vua Sandwiches has the TOS and privacy policy documents merged into one document. Hence captive-portal-links (P1) is rated as partially provided. It partially satisfies update-info-information (P2) since it includes the last update date in the privacy policy section, and at the same time, it does not notify the user with changes (similar rating for TOS P4). The hotspot collects the name, email address, phone number, and profile picture through registration form or use Facebook social login. However, the privacy policy only states that they collect the name, and social media account

details without much details on information that are shared from social media account, hence, we rate the hotspot as lacking support to report-data-collection (C2) feature. We rate Vua Sandwiches as partially satisfying PII-access-edit-delete (C6) because although it allows users to access/update PII but the policy does not specify clearly if the user can request to delete the personal information. It does not satisfy data-storage-location (S1) as PII may be maintained in Canada, the US or any other country. It also does not satisfy dedicated-privacy-support (S3) as they have a generic email address for sharing privacy concerns. The hotspot lacks no-third-party-data-sharing (D2) because the hotspot shares data with third-party captive portal. Finally, the hotspot is governed by the federal laws of the province of Ontario and the laws of Canada.

5.4 Conclusion

We outline a group of criteria for evaluating various privacy aspects in hotspots - to help us better understand if hotspot privacy policy conforms to privacy best practices and if they implement necessary technical measures to comply with them. We use our collected hotspots' datasets to validate 16 privacy policy and TOS documents from hotspots that appear to be most risky in Chapter 3. We highlight several concerns in the privacy practices of those hotspots, especially in the area of data collection, secure data transfer, data sharing, data storage location, and web tracking. We augment our policy analysis by using our collected hotspots' datasets to validate some of those privacy practices. Our analysis reveals many instances where the hotspot may appear to conform to privacy best practices

according to its documentation. but fail to implement necessary technical measures.

Chapter 6

Concluding Remarks

Many people across the world use public WiFi offered by an increasing number of businesses and public/government services. The use of VPNs, and the adoption of HTTPS in most websites and mobile apps largely secure users' personal/financial data from a malicious hotspot provider and other users of the same hotspot. However, device/user tracking as enabled by hotspots due to their access to MAC address and PII, remains as a significant privacy threat, which has not been explored thus far. Our analysis shows clear evidence of privacy risks and calls for more thorough scrutiny of these public hotspots by e.g., privacy advocates and government regulators.

In here, we provide some insightful and worthy recommendations that could protect users' privacy when using public WiFi hotspots. Our recommendations for hotspots users include the following: Users should avoid sharing any personal information with the hotspot (social media or registration forms). To reduce user tracking, users should use private browsing and possibly some other anti-tracking browser addons, and software programs

that may allow to use a fake MAC address on Windows. They should also clear the browser history after visiting a hotspot if private browsing mode is not used, and update the setting to stop automatic connection to public Wi-Fi Services. To protect personal data, users should use a VPN when connecting to a public WiFi network; or use some addons that force the browser to use encryption on captive portals that does not use HTTPS— the addons do not protect on all captive portals so users should check for https in the URL to make sure a captive portal is secure.

When connecting to public WiFi from Android, Android stores persistent cookies in the captive portal app. These cookies are not erased when the portal app is closed, or when the user leaves the hotspot. Instead, the cookies remain active as set in their validity periods. Hotspots can use these cookies to uniquely identify and authenticate user devices even when the device MAC address is dynamically changed. A better approach is to erase those cookies when the captive portal app is closed. As for device fingerprinting, Android could start blocking third-party requests to companies that are known to participate in fingerprinting users—e.g., Disconnect [17] maintains a list of companies that fingerprint users.

On Windows, the captive portal is loaded in the default regular browser and hence embedded trackers are available to all websites visited by the users. A better approach is to open the captive portal in the private browsing mode and start blocking third-party requests to companies that are known to participate in fingerprinting (e.g., Disconnect fingerprinting list [17]). Doing so not only reduces the stateful user tracking (cookie-based) but also enables users to reduce stateless user tracking (device fingerprinting) and gives users the flexibility to install some additional anti-tracking browser addons.

In what follows, we provide a summary of some possible future work directions:

- More automation. This will allow us to improve our coverage and collect/analyze data from more cities across the world.

- In our work, we provided a high-level analysis of tracking in Europe and the US public WiFi captive portals (Chapter 4). We need to consider a more in-depth study similar to our analysis to the Canadian hotspots in Chapter 3, including analysis of data collection and share practices, HTTPS adoption of captive portals, and analyze stateful or stateless tracking behaviors.

- We need to update our framework to measure device fingerprinting on Android.

- We only designed a data collection framework (`CPInspector`) for both Windows and Android. It is useful to create data collection framework for macOS and iOS. This may also help us to extend our study to provide a comparison between hotspots privacy practices on multiple platforms.

- For greater scalability (as opposed to our current manual analysis), our analytical process for evaluating hotspot privacy policies and terms of use documents needs to be automated.

Bibliography

[1] Zainul Abi Din, Panagiotis Tigas, Samuel T King, and Benjamin Livshits. {PERCIVAL}: Making in-browser perceptual ad blocking practical with deep learning. In *2020 {USENIX} Annual Technical Conference ({USENIX}{ATC} 20)*, pages 387–400, 2020.

[2] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, and Claudia Diaz. The web never forgets: Persistent tracking mechanisms in the wild. In *ACM SIGSAC Conference on Computer and Communications Security (CCS'14)*, Scottsdale, AZ, USA, November 2014.

[3] Gunes Acar, Marc Juarez, Nick Nikiforakis, Claudia Diaz, Seda Gürses, Frank Piessens, and Bart Preneel. FPDetective: Dusting the web for fingerprinters. In *ACM CCS'13*, Berlin, Germany, November 2013.

[4] Adobe Corporate Communications. Flash and the future of interactive content. Blog article (Jul. 25, 2017). https://theblog.adobe.com/adobe-flash-update.

[5] Adobe.com. Adobe experiance cloud: Device Co-op privacy control. https://cross-device-privacy.adobe.com.

[6] Adobe.com. Flash local shared objects. https://helpx.adobe.com/flash-player/kb/disable-local-shared-objects-flash.html.

[7] Aislelabs.com. Aislelabs social WiFi platform. https://www.aislelabs.com.

[8] Adam Barth. HTTP state management mechanism, 2011. RFC 6265 (Standards Track). https://tools.ietf.org/html/rfc6265.

[9] Reuben Binns, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. Measuring third-party tracker power across web and mobile. *ACM Transaction on Internet Technology*, 18(4):52:1–52:22, August 2018.

[10] Justin Brookman, Phoebe Rouge, Aaron Alva, and Christina Yeung. Cross-device tracking: Measurement and disclosures. In *Proceedings on Privacy Enhancing Technologies (PETS)*, Minneapolis, MN, USA, July 2017.

[11] Tomasz Bujlow, Valentín Carela-Español, Josep Sole-Pareta, and Pere Barlet-Ros. A survey on web tracking: Mechanisms, implications, and defenses. *Proceedings of the IEEE*, 105(8):1476–1510, 2017.

[12] Cadillacfairview.com. The Cadillac Fairview Corporation Limited. https://www.cadillacfairview.com.

[13] Ningning Cheng, Xinlei Oscar Wang, Wei Cheng, Prasant Mohapatra, and Aruna Seneviratne. Characterizing privacy leakage of public wifi networks for users on travel. In *2013 Proceedings IEEE INFOCOM*, Turin, Italy, April 2013.

[14] Cominar.com. Cominar Real Estate Investment Trust. https://www.cominar.com.

[15] Coolblue.ca. Coolblue WiFi. https://www.coolblue.ca.

[16] Crunchbase. https://about.crunchbase.com.

[17] Disconnect.me. Disconnect tracking protection lists. https://disconnect.me/trackerprotection.

[18] EasyList. https://easylist.to.

[19] Peter Eckersley. How unique is your web browser? In *International Symposium on Privacy Enhancing Technologies Symposium*, 2010.

[20] Oleg Elifantiev. NodeJS module to compare two DOM-trees. https://github.com/Olegas/dom-compare.

[21] Steven Englehardt and Arvind Narayanan. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, October 2016.

[22] Eye-In.com. Eye-in wifi. www.eye-in.com.

[23] Fpf.org. Future of privacy forum. https://fpf.org.

[24] Ftc.gov. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business. https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

[25] Alejandro Gómez-Boix, Pierre Laperdrix, and Benoit Baudry. Hiding in the crowd: an analysis of the effectiveness of browser fingerprinting at large scale. In *TheWebConf (WWW'18)*, Lyon, France, April 2018.

[26] Google. HTTPS encryption on the web. https://transparencyreport.google.com/https/overview?hl=en.

[27] Google.com. Working with IndexedDB. Progressive Web Apps Training (Apr. 11, 2018) https://developers.google.com/web/ilt/pwa/working-with-indexeddb.

[28] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G Shin, and Karl Aberer. Polisis: Automated analysis and presentation of privacy policies using deep learning. In *27th USENIX Security Symposium*, Baltimore, MD, USA, August 2018.

[29] Guy Harris. Secure Socket Layer (SSL). Wiki post (Dec 20, 2018). https://wiki.wireshark.org/SSL.

[30] Hoovers. http://www.hoovers.com.

[31] IvanhoeCambridge.com. Ivanhoe cambridge. https://www.ivanhoecambridge.com.

[32] Arjaldo Karaj, Sam Macbeth, Rémi Berson, and Josep M. Pujol. WhoTracks.Me: Shedding light on the opaque world of online tracking, 2018.

[33] Richard Klafter. Don't FingerPrint Me. https://github.com/freethenation/DFPM.

[34] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. When I am on Wi-Fi, I am fearless: privacy concerns & practices in everyday Wi-Fi use. In *SIGCHI'09*, Boston, MA, USA, April 2009.

[35] Amit Klein and Benny Pinkas. DNS cache-based user tracking. In *Network and Distributed System Security Symposium (NDSS'19)*, San Diego, CA, USA, February 2019.

[36] Pierre Laperdrix, Walter Rudametkin, and Benoit Baudry. Beauty and the beast: Diverting modern web browsers to build unique browser fingerprints. In *IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2016.

[37] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. Tranco: A research-oriented top sites ranking hardened against manipulation. In *NDSS'19*, San Diego, CA, USA, February 2019.

[38] Moustafa Mahmoud, Md Zakir Hossen, Hesham Barakat, Mohammad Mannan, and Amr Youssef. Towards a comprehensive analytical framework for smart toy privacy practices. In *Workshop on Socio-Technical Aspects in Security and Trust (STAST'17)*, Orlando, FL, USA, December 2017.

[39] Medium.com. My hotel WiFi injects ads. does yours? News article (Mar. 25, 2016). https://medium.com/@nicklum/my-hotel-WiFi-injects-ads-does-yours-6356710fa180.

[40] Microsoft.com. Basic profile fields. Online documentation (Feb. 13, 2019). https://docs.microsoft.com/en-us/linkedin/shared/references/v2/profile/basic-profile.

[41] Keaton Mowery and Hovav Shacham. Pixel perfect: Fingerprinting canvas in HTML5. *Proceedings of W2SP*, pages 1–12, 2012.

[42] Mozilla . Public Suffix List. https://publicsuffix.org/.

[43] Mozilla.org. Web storage API. MSDN Web Docs (Mar 18, 2019) https://developer.mozilla.org/en-US/docs/Web/API/Web_Storage_API.

[44] Nick Nikiforakis, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. In *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, May 2013.

[45] Council of European Union. General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[46] Łukasz Olejnik, Gunes Acar, Claude Castelluccia, and Claudia Diaz. The leaking battery. In *Data Privacy Management, and Security Assurance*, pages 254–263. Springer, 2015.

[47] PANOPTICLICK. Panopticlick website. https://panopticlick.eff.org/.

[48] PCWorld.com. Comcast's open WiFi hotspots inject ads into your browser. News article (Sep. 09, 2014). https://www.pcworld.com/article/2604422/comcasts-open-wi-fi-hotspots-inject-ads-into-your-browser.html.

[49] Charles Reis, Steven D. Gribble, Tadayoshi Kohno, and Nicholas C. Weaver. Detecting in-flight page changes with web tripwires. In *NSDI'08*, San Francisco, CA, USA, 2008.

[50] Norman Sadeh, Alessandro Acquisti, Travis D Breaux, Lorrie Faith Cranor, Aleecia M McDonald, Joel R Reidenberg, Noah A Smith, Fei Liu, N Cameron Russell, Florian Schaub, et al. The usable privacy policy project. *Technical report, Technical Report, CMU-ISR-13-119*, 2013.

[51] Iskander Sanchez-Rola and Igor Santos. Knockin'on trackers' door: Large-scale automatic analysis of web tracking. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 281–302. Springer, 2018.

[52] Iskander Sanchez-Rola, Igor Santos, and Davide Balzarotti. Clock around the clock: Time-based device fingerprinting. In *ACM CCS'18*, Toronto, Canada, October 2018.

[53] Anastasia Shuba and Athina Markopoulou. Nomoats: Towards automatic detection of mobile tracking. *Proceedings on Privacy Enhancing Technologies*, 2020(2):45–66, 2020.

[54] Nissy Sombatruang, Youki Kadobayashi, M. Angela Sasse, Michelle Baddeley, and Daisuke Miyamoto. The continued risks of unsecured public WiFi and why users keep using it: Evidence from Japan. In *Privacy, Security and Trust (PST'18)*, Belfast, UK, August 2018.

[55] Sy5.ca. Sy5 wifi. https://sy5.ca.

[56] Symantec. Norton WiFi risk report: Summary of global results. Tech report (May 5, 2017). https://www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.pdf.

[57] Giorgos Tsirantonakis, Panagiotis Ilia, Sotiris Ioannidis, Elias Athanasopoulos, and Michalis Polychronakis. A large-scale analysis of content modification by open HTTP proxies. In *Network and Distributed System Security Symposium (NDSS'18)*, 2018.

[58] Pelayo Vallina, Álvaro Feal, Julien Gamba, Narseo Vallina-Rodriguez, and Antonio Fernández Anta. Tales from the porn: A comprehensive privacy analysis of the web porn ecosystem. In *Proceedings of the Internet Measurement Conference*, pages 245–258, 2019.

[59] Valve. Fingerprintjs by Valve. https://valve.github.io/fingerprintjs/.

[60] Webpolicy.org. AT&T hotspots: Now with advertising injection. News article (Aug. 25, 2015) http://webpolicy.org/2015/08/25/att-hotspots-now-with-advertising-injection.

[61] Wireshark.org. Tshark - Dump and Analyze Network Traffic. Online documentation (Mar. 2019). https://www.wireshark.org/docs/man-pages/tshark.html.

[62] Zhiju Yang and Chuan Yue. A comparative measurement study of web tracking on mobile and desktop environments. *Proceedings on Privacy Enhancing Technologies*, 2:24–44, 2020.

[63] YelpWiFi.com. Yelp WiFi. https://www.yelpWiFi.com.

Appendix A

List of Persistent Cookies

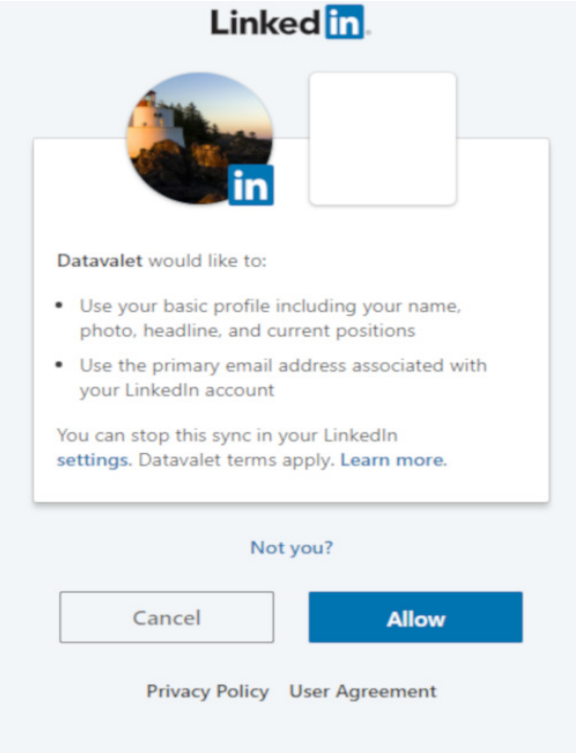
Table 14: List of persistent cookies valid for five years of more.

Hotspot	Scope	Third-Party	Tracker	Base-Domain	Name	Years
CF Carrefour Laval	Captive Portal	Yes	No	network-auth.com	p_session_id	20
CF Fairview Pointe Claire	Captive Portal	Yes	No	network-auth.com	p_session_id	20
CHU Sainte-Justine	Landing Page	No	No	chusj.org	VisitorStatus	20
CIBC Bank	Landing Page	Yes	Yes	stackadapt.com	sa-user-id-v2	5
CIBC Bank	Landing Page	Yes	Yes	stackadapt.com	sa-user-id	5
CIBC Bank	Landing Page	No	No	cibc.com	atgRecVisitorId	19
Carrefour Angrignon	Captive Portal	Yes	No	google.ca	CONSENT	19
Carrefour Angrignon	Captive Portal	Yes	No	google.com	CONSENT	19
Discount Location d'Auto	Landing Page	Yes	No	wayfair.com	CSNBrief	10
Discount Location d'Auto	Landing Page	Yes	No	wayfair.com	CSNUtId	10
Fido	Landing Page	No	No	fido.ca	ClicktaleReplayLink	81
Fido	Landing Page	No	No	fido.ca	optimizelyBuckets	10
Fido	Landing Page	No	No	fido.ca	optimizelySegments	10
Fido	Landing Page	No	No	fido.ca	optimizelyEndUserId	10
Fido	Landing Page	No	No	fido.ca	language	68
Fido	Landing Page	No	No	fido.ca	province	68
Fido	Landing Page	No	No	fido.ca	TLTUID	10
Fossil	Landing Page	Yes	No	pbbl.co	pp_uid	25
Fossil	Landing Page	No	No	fossil.com	_br_uid_2	99
Fossil	Landing Page	No	No	fossil.com	s_fid	5
GAP Brands	Landing Page	No	No	gapcanada.ca	s_chan	5
GAP Brands	Landing Page	No	No	gapcanada.ca	s_fid	5
Harvey's	Landing Page	No	No	harveys.ca	optimizelyEndUserId	10
Harvey's	Captive Portal	Yes	No	network-auth.com	p_session_id	20
Harvey's	Landing Page	No	No	harveys.ca	optimizelyDomainTestCookie	10
Hvmans Cafe	Captive Portal	Yes	No	instagram.com	mid	10
Hvmans Cafe	Captive Portal	Yes	No	instagram.com	mcd	10
Ikea	Landing Page	No	No	ikea.com	s_pers	5
Ikea	Landing Page	No	No	ikea.com	s_fid	5
Juliette Et Chocolat	Landing Page	No	No	julietteetchocolat.com	secure_customer_sig	20
Laura	Landing Page	No	No	laura.ca	liveagent_ptid	10
Laura	Landing Page	No	No	laura.ca	liveagent_vc	10
Laura	Landing Page	No	No	laura.ca	liveagent_oref	10
Laura	Landing Page	No	No	laura.ca	optimizelyBuckets	10
Laura	Landing Page	No	No	laura.ca	optimizelySegments	10
Laura	Landing Page	No	No	laura.ca	optimizelyEndUserId	10
McDonald's	Captive Portal	Yes	No	network-auth.com	p_session_id	20
Pizza Pizza	Landing Page	Yes	No	intentiq.com	AWSELB	10
Pizza Pizza	Landing Page	Yes	No	intentiq.com	IQPData	10
Pizza Pizza	Landing Page	Yes	No	intentiq.com	intentIQ	10
Pizza Pizza	Landing Page	Yes	No	intentiq.com	ASDT	10
Pizza Pizza	Landing Page	Yes	No	intentiq.com	CSDT	10
Pizza Pizza	Landing Page	Yes	No	intentiq.com	intentIQCDate	10
Pizza Pizza	Landing Page	Yes	No	intentiq.com	IQver	10
Place Montreal Trust	Captive Portal	No	No	placemontrealtrust.com	welcome_info_name	5
Place Montreal Trust	Captive Portal	No	No	placemontrealtrust.com	expected_tab	5
Roots	Landing Page	Yes	No	instagram.com	mid	10
Roots	Captive Portal	Yes	No	instagram.com	mcd	10
Roots	Captive Portal	Yes	No	network-auth.com	p_session_id	20
ScotiaBank	Landing Page	No	No	scotiabank.com	site	20
TD Bank	Landing Page	No	No	td.com	s_pers	5
TD Bank	Landing Page	Yes	No	owneriq.net	si	5
Tim Hortons	Captive Portal	Yes	No	network-auth.com	p_session_id	20
Via Rail Station	Captive Portal	Yes	No	network-auth.com	p_session_id	20
Walmart	Landing Page	No	No	walmart.ca	btc	10
Walmart	Landing Page	No	No	walmart.ca	vtc	10
Walmart	Landing Page	No	No	walmart.ca	og_session_id	20
Walmart	Landing Page	No	No	walmart.ca	walmart.id	9

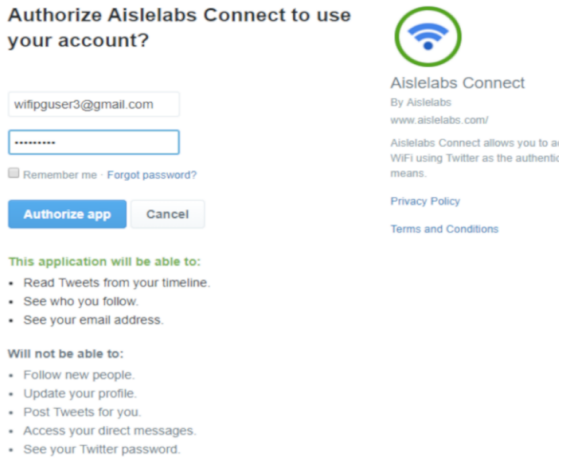
Appendix B

Examples of Social Media Use

In here, we provide examples of social login messages presented to the user requesting permissions to access the data.

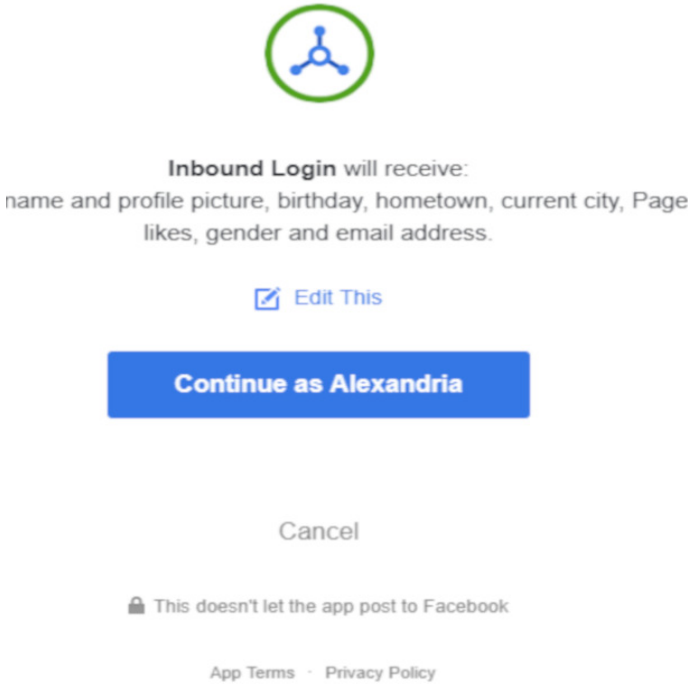


(a) LinkedIn

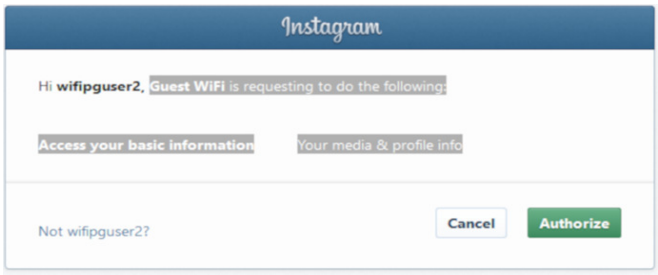


(b) Twitter

Figure 8: Examples of social login messages presented to the user from LinkedIn and Twitter. (Images quality is limited because they were automatically captured by our data collection framework which depends on the resolution supported by Selenium).



(a) Facebook



(b) Instagram

Figure 9: Examples of social login messages presented to the user from Facebook and Instagram. (Images quality is limited because they were automatically captured by our data collection framework which depends on the resolution supported by Selenium).

Appendix C

List of Evaluated Hotspots Worldwide

Table 15: List of evaluated hotspots from Canada.

Category	Region	Count	Hotspot Name
Retail business	Ontario	16	Anthropologie, MAC Cosmetics, NYX, Roots, Sephora, Spence Diamonds, Vans, Bluenotes, Brisk, Gap, H&M, Laura, LCBO, The Childrens Place, Tip Top, Walmart
Cafe and Restaurant	Ontario	9	McDonald's, ONroute, A&W Restaurants, The Second Cup, Sobeys, South St. Burger, Starbucks, Subway, Tim Hortons
Telecom Kiosk	Ontario	3	Fido, Rogers, Telus
Bank	Ontario	2	National Bank of Canada, TD Bank
Shopping Mall	Ontario	2	Rideau Centre, Bayshore
Hairdresser	Ontario	1	First Choice Haircutters
Cafe and Restaurant	Quebec	19	Copper Branch, Bombay Mahal Thali, Hvmans Cafe, Pizza Pizza, Vua Sandwiches, Sushi STE-Catherine, Cafe Osmo, The Second Cup, A&W Restaurants, Domino's Pizza, Juliette Et Chocolat, Burger King, McDonald's, Starbucks, Tim Hortons, Harvey's, Moose BAWR, Pizza Hut, Nespresso
Retail business	Quebec	17	GAP, Dynamite, Fossil, Ikea, Laura, SAQ, Maison Simmons, Roots, Walmart, H&M, Home Depot, Canadian Tire, Garage, IGA, ECCO, Michael Kors, Sephora
Shopping Mall	Quebec	12	Complexe Desjardins, Carrefour iA, Place Montreal Trust, Place Vertu, Centre Eaton, Fairview Pointe-Claire, Carrefour Angrignon, Carrefour Laval, Mail Champlain, Place Ville Marie, Atrium 1000, Centre Rockland
Bank	Quebec	5	RBC Bank,TD Bank, ScotiaBank, CIBC Bank, Desjardins 360
Art and Entertainment	Quebec	4	Place Des Arts, Grevin Montreal, YMCA, Montreal Science Centre
Transportation	Quebec	3	Gare d'autocars de Montréal, Via Rail Station, YUL Airport
Telecom Kiosk	Quebec	2	Fido,Telus
Car Rental	Quebec	1	Discount Car Rental
Gymnasium	Quebec	1	Nautilus Plus
Hospital	Quebec	1	CHU Sainte-Justine
Hotel	Quebec	1	Fairmont Hotel
Library	Quebec	1	Westmount Public Library

Table 16: List of evaluated hotspots from Europe.

Category	Region	Count	Hotspot Name
Retail business	Luxembourg	18	Arket, Auchun, Cactus, Cartier, CHANEL, Cora, COS, Ernster, Gucci, H&M, Jack & Jones, Louis Vuitton, MAC Cosmetics, Other Stories, Paris XL, Veritas ,A.S Adventure, Weekdays
Cafe and Restaurant	Luxembourg	12	Brochettes et Cie, Burger King, Chi-Chis, EXKI Wifi, Fischer, KIKI, Laudree, Namur, Pizza Hut, Rock Box, Victorine, Zulu
Shopping Mall	Luxembourg	4	City Concorde, Cloche d'Or, Galerie Auchan Kirchberg, La Belle Etoile
Bank	Luxembourg	2	BCEE,ING
City WiFi	Luxembourg	2	CityWiFi, VDL
Transportation	Luxembourg	2	Central Station, Luxembourg Airport
Hotel	Luxembourg	1	DoubleTree Hilton
Other	Luxembourg	1	Orderbird AG
Transportation	Netherlands	2	Schiphol Airport, Amsterdam Central Station
Hotel	Netherlands	1	The Manor Amsterdam-NL
Transportation	France	2	Paris Airport, My Paris Airport

Table 17: List of evaluated hotspots from the US.

Category	Region	Count	Hotspot Name
Cafe and Restaurant	New York	10	Andersons, Burger King, Dunkin Donuts, Chili's, McDonald's, Old Country Buffet, Starbucks, Taco Bell,Tim Hortons, Tinder Box
Retail business	New York	9	Barnes & Noble, Bed Bath & Beyond, Best Buy, Famous Footwear, Lowe's, Petco, Michaels, Party City, Lowes
Art and Entertainment	New York	2	Niagara Falls State Park, Maid of the Mist Boat Tour
Bank	New York	2	M&T Bank, Key Bank
Auto Repair	New York	1	Firestone Complete Auto Care
Hotel	New York	1	Super 8
Telecom Kiosk	New York	1	Spectrum

Appendix D

Hotspots Privacy Policy Links

Table 18: Links to evaluated hotspots' privacy policies and terms of service.

Product	Policy link	Terms of Service
Bombay Mahal Thali	https://sy5.ca/en/terms/	
CF Carrefour Laval	https://www.cadillacfairview.com/en_CA/privacy.html	https://splash.aislelabs.com/o/portal/swtc_20.jsp
CF Fairview Pointe Claire	https://www.cadillacfairview.com/en_CA/privacy.html	https://passs.net/o/portal/swtc_20.jsp
Carrefour Angrignon	https://login.eyeintelligence.com/terms/termsofuse.php?lang=EN&dealerid=carrefourangrignon#PrivacyPolicy	https://login.eyeintelligence.com/terms/termsofuse.php?lang=EN&dealerid=carrefourangrignon
Centre Eaton	https://www.centreeatondemontreal.com/en/privacy-policy/	https://www.centreeatondemontreal.com/en/wifi-terms-conditions/
Centre Rockland	https://login.eyeinwireless.com/terms/termsofuse.php?lang=EN&dealerid=centrerockland#PrivacyPolicy	https://login.eyeinwireless.com/terms/termsofuse.php?lang=EN&dealerid=centrerockland
Domino's Pizza	https://www.dominos.ca/#/content/privacy/?lang=en	https://caservice.dominos.ca/dominoscanadaapi/wifiPortal/portal?lang=en
Dynamite*	https://www.dynamiteclothing.com/ca/community/privacy-policy(*)	http://wifi.dynamite.ca/ca-en/agreement_view.html
Garage*	https://www.garageclothing.com/ca/community/privacy-policy(*)	http://wifi.garage.ca/ca-en/agreement_view.html
Grevin Montreal	https://login.eyeinwireless.com/terms/termsofuse.php?lang=EN&dealerid=museegrevin#PrivacyPolicy	https://login.eyeinwireless.com/terms/termsofuse.php?lang=EN&dealerid=museegrevin
Hvmans Cafe	https://region1.purpleportal.net/access/agreement/privacy-full	https://region1.purpleportal.net/access/agreement/terms
Mail Champlain	https://login.eyeinwireless.com/terms/termsofuse.php?lang=EN&dealerid=MailChamplain#PrivacyPolicy	https://login.eyeinwireless.com/terms/termsofuse.php?lang=EN&dealerid=MailChamplain
Moose BAWR	http://stickywifi.com/cp/msc/PrivacyPolicyEng2-17-2017.pdf	http://stickywifi.com/cp/msc/TermsOfServiceEng2-17-2017.pdf
Nautilus Plus*	https://www.nautilusplus.com/privacy-policy/ (*)	No online copy is available
Place Montreal Trust	https://www.placemontrealtrust.com/en/privacy-policy/	http://www.placemontrealtrust.com/en/socialwifi-terms-conditions/
Roots	https://www.yelpwifi.com/privacy-policy	https://www.yelpwifi.com/terms-of-service
Sushi STE-Catherine	https://www.mywifi.io/page/privacy	No online copy is available
Vua Sandwiches	https://www.coolblue.ca/privacypolicy	https://www.coolblue.ca/terms-and-conditions

(*) = There is no link to the document from the captive portal.