Reflection: Is Browser Fingerprinting Flying Under the Regulatory Radar?

By: Zhuzhen Li (1002066328) and Ethan Blumberg (1009915479)

Word Count: 1195

Part 1: Introduction

Browser Fingerprinting is a digital tracking technique that embodies a key struggle in Canadian privacy regulation; can privacy law and enforcement keep up with digital innovation? Browser fingerprinting was originally deployed for security purposes but now has become a way to strategically track user identities. Our group was shocked to find out how a systematic collection and use of data by companies seems to avoid a high level of regulatory scrutiny. However, upon further investigation, we realized the data collected does not always fall within the conventional definition of "personal information" [1]. Our conversation then quickly turned to whether such information in our new digital age should be regulated and can be considered "personal".

We are no longer in the era of contemplating how patient registration forms should be regulated [2]. Decades of rapid innovation have led to a whole new set of private information that can be of value. Particularly individuals' digital fingerprints are highly valuable and allow private companies to identify and track user behaviour. Browser fingerprinting tracks data such as time zones, installed plug-ins and the type of hardware device, creating a digital fingerprint of the user. However, it seems companies have managed to excuse themselves from adhering to privacy regulations due to the technical focus of the data. Our reflection hopes to investigate browser fingerprinting and explore the technology behind it. We will also briefly examine the underlying question of whether privacy regulators are able to effectively keep up with emerging tracking technologies.

Part 2: Legal Analysis

At the core of contemporary Canadian privacy regulation is the idea of consent [2]. However, if Canadian privacy law does not deem information "personal" individuals will not have to provide consent for the commercial use of their data by private entities under PIPEDA. Through this class, we have analyzed privacy by considering if an individual has been able to meaningfully consent to the "collection, use and disclosure" of their personal information [2]. However, to our groups surprise organizations will utilize browser fingerprinting and seemingly disregard obtaining consent.

Browser fingerprinting allows private actors to create highly unique identities without relying on cookies. The fact that browser fingerprinting is not highly scrutinized seems at odds with privacy law jurisprudence and PIPEDA. Being able to track an individual's use of the internet and specific details about their use seems highly personal in nature. Personally we believe companies manage to get away with it because it has not been deemed a pressing issue against personal

privacy such as cookies. With so much of our life spent online, being precisely tracked should be characterized as personal and like cookies should face intense regulatory scrutiny.

While Canadian federal privacy experts spent years developing a way to regulate and enforce against cookies, large tech companies have pivoted to a more discrete way to track internet users. Browser fingerprinting is just one of many examples of when the power, expertise and resources of private companies make it far too difficult for Canadian authorities to explore, regulate and enforce privacy infringements. In the post-cookie era, it seems like companies are looking for new and innovative ways to track users that fall in line with regulations, or like fingerprinting can hide under the radar of regulatory bodies.

Part 3: Technical Analysis and Ambiguity

As an alternative method to obtain PII rather than traditional cookies, browser fingerprinting is a more advanced tracking technique that identifies users based on unique device and browser attributes. When a webpage is rendered on the user's browser, scripts such as JavaScript are executed within the webpage. This is the time when the code is collecting a variety of data points about hardware and software characteristics. These hundreds of signals include details about the browser environment, operating system configurations, network properties, behavioral patterns. Since each browser and device combination exposes slightly different responses to web-based queries, these attributes can be processed into a high-entropy, near-unique fingerprint identifier for every single device [3].

Canvas Fingerprinting is a popular tracking technique which utilizes the HTML5 <canvas> element to draw invisible text or images. Next it measures pixel-level variations caused by differences in GPU hardware, rendering algorithms, sub-pixel anti-aliasing methods, and system font rendering settings, uniquely identifying each device based on how it renders images [4]. Although these differences are undetectable to humans, a script can easily extract the accurate pixel values and hash them into a unique identifier [4]. In addition, to further refine user identification, the fingerprinting technique is able to gather personal information such as font enumeration, time zone, and network protocol and conduct installed browser plugin analysis [5].

Fingerprinting is significantly harder to detect and prevent. Since it does not rely on data storage on the user's browser, the opt-out solution for cookies is ineffective for it. Private browsing modes like Chrome's Incognito Mode or Firefox's Private Browsing, cannot prevent fingerprinting either [6]. This is because the collected device information like GPU model, screen resolution, and font settings, are consistent across the browsing sessions no matter whether private mode is being used or not. Moreover, modern fingerprinting techniques use machine learning models to detect behavioral patterns, including but not limited to mouse movement speed, typing cadence, and scrolling behavior. This further enhances the fingerprinting identification accuracy, because this diverse and highly informative dataset helps the training of machine learning models to differentiate between users [7]. Fingerprinting is operating at scale across advertising networks, analytics platforms, and fraud detection systems, often without users realizing they are being tracked. As an exceptionally effective and difficult-to-detect tracking method in modern web environments, fingerprinting's persistence is a significant concern due to its ability to track internet users.

However, countermeasures are emerging to lower the fingerprinting risks. Privacy-focused browsers, such as Brave and Tor, use fingerprint randomization, which changes JavaScript-reported values for certain system attributes on each browsing session, making it harder for trackers to generate stable identifiers [9]. Firefox's Enhanced Tracking Protection (ETP) and Apple's Safari Intelligent Tracking Prevention (ITP) actively limit the amount of readable system data available to websites [10]. In addition, privacy extensions such as uBlock Origin and Privacy Badgerc cannot prevent all types of tracking; they still attempt to block known fingerprinting scripts [10]. However, main browser companies do not have sufficient incentives to invest in the technical development of anti-fingerprinting technology. For example, Google Chrome has deep financial ties to the online advertising business, where fingerprinting plays a crucial role in user tracking and targeted advertising.

Part 4: Conclusion

Fingerprinting is on pace to become a prominent tracking method in the post-cookie era and brings significant challenges for privacy authorities in Canada. GDPR and PIPEDA are expected to set reasonable regulations with feasible enforcement for fingerprinting which cannot be bypassed. However, the discrete nature and technical focus of fingerprinting make it a hard issue to resolve. Even when the countermeasures exist, the lack of regulatory scrutiny significantly limits the regulation of user tracking through fingerprinting. The legal and technical limitations highlight the growing gap between privacy laws and tracking technology. We are looking forward to seeing stronger legal enforcement, industry standards, and user-driven privacy tools to achieve a balance between tracking and user privacy rights.

References:

[1] Austin, L., & Lie, D. (2025). Lecture 5: Privacy problems [PowerPoint slides]. Privacy Problems, University of Toronto

[2] Austin, L., & Lie, D. (2025). Lecture 2: Privacy problems [PowerPoint slides]. Privacy Problems, University of Toronto

[3] CJEU, "Judgment of the Court (Grand Chamber) of 1 October 2019," Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH, Case C-673/17. [Online]. Available: CJEU Planet49 Case.

[4] Cookiebot, "What is the ePrivacy Regulation?" [Online]. Available: Cookiebot ePrivacy.

[5] Office of the Privacy Commissioner of Canada, "Policy Position on Online Behavioural Advertising," [Online]. Available: OPC Tracking & Ads.

[6] EDPB, "Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive," European Data Protection Board, Nov. 2023. [pdf].

[7] European Parliament, “Directive 2009/136/EC on Privacy and Electronic Communications,” Official Journal of the European Union, 25 Nov. 2009. [pdf].

[8] Bahrami, P. N., Iqbal, U., & Shafiq, Z. (2021). “FP-Radar: Longitudinal Measurement and Early Detection of Browser Fingerprinting,” arXiv preprint arXiv:2112.01662.

[9] Iqbal, U., Englehardt, S., & Shafiq, Z. (2020). “Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors,” arXiv preprint arXiv:2008.04480.

[10] Sundaram Muthu Selva Annamalai, M., Bilogrevic, I., & De Cristofaro, E. (2023). “FP-Fed: Privacy-Preserving Federated Detection of Browser Fingerprinting,” arXiv preprint arXiv:2311.16940.