Katharine Chi
Professor Smith
WRIT 159A
31 January 2025

Science Vs. Incognito Mode

In the age of rapid technological development, privacy becomes a top concern of the public realm. With long-winded and complicated disclosures, there are valid concerns over how one interacts with the internet and what information is disseminated without explicit permission. Users have available on mobile devices and computers the option of "Incognito Mode", and most perceive this mode of private browsing as "safer" and just enough for the conscious to feel secure. In a public forum on Quora, one user commented[1], "Browsing in Incognito mode will keep your internet activity private. Nothing you do in Incognito mode will be stored in your history or phone."

Incognito mode is a feature of Google Chrome and other web browsers that allows users to browse the internet without saving browsing history, cookies, and other data. The browser does not save the websites visited in the closed session. Most browsers offer some form of a private browsing feature, whether it is Safari's "Private browsing" or Firfox's "Private mode". Private browsing was intentionally[2] made for those who want to separate their work and personal life, those who share a device with other users, those who are buying a surprise gift, and those who may just want to limit the amount of information companies collect. Web tracking[2] is a major cause of privacy concerns, as many sites utilize browsing activity to understand how interested the user would be in purchasing a specific product or clicking on an article. In addition to gauging the user's preferences and interests, web tracking is used to improve the overall site experience. Most tracking is used to provide ads, and they are often catered to one's browser activity. If a user has been looking through the internet for a new jacket, various ads about jackets on sale will 'coincidentally' appear typically through browser cookies. After visiting a site, the advertiser leaves a tracking cookie[3] on the user's browser, which takes the form of a unique ID. The cookies, containing the user's information and ID, are stored in the cloud folder, and includes which sites were visited, how long each site session was, what was clicked on, and what language preferences were set. Web browsers attach relevant cookies to any future requests made on the web server, allowing websites to personalize the user's experience. Tracking cookies can also report data to social sites such as Instagram, which is why ads will sometimes follow users into social media.

So how does incognito mode affect this data collection frenzy? Choosing to browse privately, cookie data and tracking cookies are deleted from the local device[4] when the user closes the window. Downloaded files are also not remembered by the browser, but still exist in the computer files. Without this saved data, the user's session is not visible to others using the same device and ads based on the closed signed-out session cannot be provided. However, while the user history is not saved and cookies are deleted, the IP address is visible and websites can

still collect data during the active session through other tracking mechanisms[5]. In spite of being in incognito mode, user activity is collected[6] by web browsers and sites in an aggregated or anonymized system. The crucial fine print to private browsing and incognito mode is the scale of anonymity and the complexity of data collection. Although an appealing name, incognito mode is not the do-all solution to data security.

To understand why people use incognito mode, a study at Carnegie Mellon University[7] observed daily browsing activity and behavior using a survey with over 450 participants. Many of the responses explained using private browsing for practical and privacy-sensitive activities. The participants were generally concerned with other users viewing their online activity, but also expected protection from web tracking and targeted advertising. Two-thirds of responses overestimated the protections included in this browsing mode, assuming that private browsing prevents websites and advertisers from tracking user data, and hides web queries from search engines. Another perceived benefit of private browsing was the protection against viruses, malware, and hacking. In around 10% of the responses, participants reported not really knowing what private browsing protected them from, but used it because it provided a feeling of security and privacy.

So, how trustworthy is private browsing? Researchers at Edinburgh Napier University[8] tested how successfully incognito mode achieved its marketed claim, and the results did in fact show that browsing activity and cookies were not being saved to the device's hard disk. All the claims made by the web browser were met. However, using volatile memory analysis, a majority of the test case data could still be retrieved. The hard disk does not save the user's data, but the random access memory of the computer stores the data until the device is completely shut down. So with the same approach, a potential attacker has the ability to access private information left on a device without the user's consent. Choosing the words, "Incognito" and "Private", to label this mode of browsing, who can blame users from assuming data security? Without a clear idea on internet privacy, incognito mode can only provide a false sense of security.

A case that captures the social turmoil surrounding data privacy is the 2020 class-action lawsuit[9] against Google. The case was a result of collecting personal and sensitive data from users that had browsed the internet using incognito mode. Google leveraged this data to measure website traffic and sell advertisements. As a result of this data collection, Google has reaped billions of dollars in profit. An engineer wrote[10] to colleagues at Google, "We need to stop calling it incognito and stop using a Spy Guy icon". There are great limitations to private browsing, yet people still continue to use this mode because the disclosure's language and design is misleading. Privacy disclosures can be long winded documents, consisting of fine print text and language that can be more intimidating than informative for the average user.

Especially with the fast-developing cultural landscape of information dissemination, disclosures and technical communications are crucial to accurately reflecting the technical logistics of data privacy. In a study conducted at University of Chicago[11] with 460 participants, each individual was shown an in-browser disclosure for one of thirteen of the most popular web browsers, and was asked twenty scenario questions in order to capture documented

misconceptions. The results showed that all tested in-browser explanations of private browsing mode failed to correct important misconceptions. Based on the tested scenarios, 56% of the participants believed that private mode web queries would not be saved while being logged into a Google account, and 27.1% believed the mode offered protections against viruses and malware. Common beliefs across the participants were that private mode protects users from viruses, and prevents websites and network providers from tracking geolocations and advertisements. One participant commented, “it’s a no brainer really, when in private mode nothing is stored.”

Clear technical language is crucial for user safety and data security. Participants who read certain disclosures had higher rates of misconceiving the abilities of private browsing and the lack thereof. The study showed a correlation between vague statements and poor-performing disclosures. Overall, the word, “Private”, is heavily generalized, and the results showed how the name of private browsing modes implies unintentional meanings. Especially when users are marketed to browse privately, participants are more so inclined to rely on their broader conceptualizations of privacy. Incognito mode and private browsing do have a certain degree of anonymity, but the gap in knowledge is rooted in poor usable privacy. With misleading labels and statements of protection such as Firefox Focus’s “browse like no one’s watching”, the usability of the security feature is detrimental to the original intentions of the developers.

Google’s marketing chief, Lorraine Twohill[10], stated, “We are limited in how strongly we can market incognito because it's not truly private, thus requiring really fuzzy, hedging language that is almost more damaging.” Acknowledging the misleading nature of incognito mode and other private browsers, companies in the information technology industry are faced with a limbo between user data profits and the standardization of user-friendly security disclosures. Engineers have also acknowledged that the name of private browsing mode is not an accurate representation of the actual benefits, thus suggesting a change in name or complete removal of the mode itself.

Legal cases over data privacy, such as Google’s class-action lawsuit, are becoming more prevalent and it begs the question of how to protect users and bridge the gap in knowledge. The misconceptions around private browsing are influenced by inadequate education on how data collection works, vague marketing language, and poor usable security, but that is not to say corporations and the government do not have the power to regulate technical communications and uphold information privacy.

Other than incognito mode, there are various avenues of building protection against invasive data collection. While private mode does clear the user’s session history from the browser, the internet provider can still view online activity, read emails, view the device geolocation, and watch video chats. Even the most credible browsers like DuckDuckGo[6] encrypt web activity only for the browser itself, and not across the entire device. Contrastingly, virtual private networks[6] (VPNs) hide the browsing history for the entire device, regardless of which browser or app is used. VPNs work by encrypting web activity and changing the IP address, so cookies and user data cannot be tracked. Before the internet activity leaves your device, the VPN encrypts the data so neither your router nor your internet provider can see the content. In addition

to utilizing a VPN, there are other precautionary approaches to web surfing such as opting out of cookies and data-sharing, turning off location sharing, and limiting app permissions. So, despite the 'Spy Guy' on your web browser page claiming to hide your activity from the digital world, your data is more vulnerable than meets the eye. In today's landscape of technology, a careful interdisciplinary approach to information privacy is imperative for truly protecting your personal data.

References

1. "Why do people use incognito mode?," *Quora*, 2019. https://www.quora.com/Why-do-people-use-incognito-mode (accessed Jan. 30, 2025).
2. "Incognito browser: What it really means," *Mozilla*. https://www.mozilla.org/en-US/firefox/browsers/incognito-browser/
3. CloudFlare, "What are cookies? | Cookies definition," *Cloudflare.com*, 2024. https://www.cloudflare.com/learning/privacy/what-are-cookies/
4. "How Chrome Incognito keeps your browsing private - Google Chrome Help," *support.google.com*. https://support.google.com/chrome/answer/9845881?hl=en#zippy=%2Chow-incognito-mode-works%2Chow-incognito-mode-protects-your-privacy
5. L. Banks, "How Are Cookies Managed in Incognito Browsing?," *Cookie Law Info*, Nov. 08, 2024. https://www.cookielawinfo.com/incognito-cookies/ (accessed Jan. 30, 2025).
6. "The Complete Guide to Private Browsers," *Security.org*. https://www.security.org/vpn/private-browsers/
7. H. Habib *et al.*, "Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing," 2018. Available: https://www.usenix.org/system/files/conference/soups2018/soups2018-habib-prying.pdf
8. K. Hughes, P. Papadopoulos, N. Pitropakis, A. Smales, J. Ahmad, and W. J. Buchanan, "Browsers' Private Mode: Is It What We Were Promised?," *Computers*, vol. 10, no. 12, p. 165, Dec. 2021, doi: https://doi.org/10.3390/computers10120165.

9. “Amended Google Complaint,” *Documentcloud.org*, 2024. https://www.documentcloud.org/documents/24527422-amended-google-complaint/ (accessed Jan. 30, 2025).
10. B. Allyn, “Google to delete search data of millions who used ‘incognito’ mode,” *NPR*, Apr. 2024. https://www.npr.org/2024/04/01/1242019127/google-incognito-mode-settlement-search-history
11. Y. Wu, P. Gupta, M. Wei, Y. Acar, S. Fahl, and B. Ur, “Your Secrets Are Safe: How Browsers’ Explanations Impact Misconceptions About Private Browsing Mode,” doi: https://doi.org/10.1145/3178876.3186088.