SHORT PIECE

Privacy Focused Companies, How Focused Are They?

By BRIAN KRUPP and JULIA GERSEY

Keywords: information privacy, information tracking, trust, application transparency
Categories: • Security and Privacy → Human and societal aspects of security and privacy

Consumers can use a variety of products and services at zero monetary cost. These services can include email, photo storage, social networking, searching the world wide web, and much more. While these services provide real value without requiring a monetary payment, many consumers give up privacy that allows these services to be funded through targeted advertising. As consumers have become more aware of how invasive these practices can be, there have been more privacy focused alternatives created. For example, instead of using Google, consumers can use privacy focused alternatives such as DuckDuckGo, Brave Search, and Ecosia. Similarly, instead of using Gmail, users can instead use ProtonMail where they claim that "privacy and freedom come first". But, how do we ensure these companies intentions match their actions? If their actions do not match their intentions, what effect can this have on consumers that choose to use these alternatives from mainstream services with a goal to protect their privacy? Recently, there have been issues raised with these services that may cause concern for consumers and a lack of trust in these alternatives.

DuckDuckGo is one of the more popular privacy-focused companies where its flagship product is their search engine. The search engine serves advertisements based on what you search at that moment in time, instead of tracking you and your search history. In their about page, they include the following: "For everyone who's had enough of online tracking, DuckDuckGo lets you take back your online privacy now." . Not only does DuckDuckGo have a search engine, [1] but they also have privacy-focused browsers. However, even with this focus on privacy, recently DuckDuckGo was found that they use the Bing search engine that is owned by Microsoft and through their agreement with Microsoft, they were not blocking all trackers as they stated and did not block Microsoft owned trackers. This includes domains such as workplace.com which is owned by Facebook . The CEO of DuckDuckGo described that this [2] was due to a non-disclosure agreement (NDA) with Microsoft and they were actively working to change these requirements. However, even with trying to remedy this lack of transparency, users of the service were told that trackers were blocked without exception.

Proton is another privacy-focused company that offers several services including email, VPN, and cloud storage. Their most popular service, ProtonMail advertises the following: "Secure email that protects your privacy. Keep your conversations private." . Their email service offers a [3] free plan where users can send a limited number of messages a day with a limited number of total storage. While they advertise privacy, in 2021 it was discovered that they shared IP address logs to French authorities through a Europol request. Previous to this discovery, they [4] advertised that they "do not keep any IP logs". However, since this finding, that claim can no longer be found on their website. Proton did try to explain the event on their blog where they state: "Proton can be forced to collect information on accounts belonging to users under Swiss criminal investigation" [5]. From this event, they do recommend users use a VPN service such as Tor to help protect themselves and they also publish an annual transparency report. However, in this transparency report it is clear that even though Proton will contest user data requests, they comply with a large portion of these requests where in 2021 they received 6,243 legal orders and complied with 4,920. While they link the transparency report that details these [6] request from their website, on the page where the email service is provided, it is a small link in the footer. Increasing this transparency with the users up front on the page of their product offering can help build trust with the users.

With the launch of iOS 14.5, Apple introduced its limited ad tracking. This new feature, called App Tracking Transparency (ATT), allowed users to select how their data could be used with advertising and helped Apple promote privacy as a core feature of their products. Yet, research done by developers at the software company Mysk has come to light and shown that Apple still collects data despite the specified user settings. The study found that Apple Music, Apple TV, Books, the iTunes Store, and Stocks, despite the user's settings, "shared consistent ID numbers, which would allow Apple to track your activity across its services" . Reinhold Kesler, [7] a researcher at the University of Zurich in Switzerland, explains how ATT helps Apple: "The feature led some app developers to shift business models from being free but with ads to paid models, sometimes including in-app payments. That was to the benefit of Apple, which takes a 30 percent cut of such payments…". From a company that advertises privacy as a core feature, Apple has shown a contradicting focus as they increased in hiring in advertising and their revenue continues to grow from it. "Apple's ad adventure risks irking loyal customers. Pushing paid messages on people is a break from the company's usual pact with consumers, who have been trained over decades to pay steep prices for Apple products that present a refined, if closed-off, experience." . So, is Apple promoting privacy with ATT for the users sake 8 or to capitalize from the feature to increase revenue?

Even with these for-profit companies lacking transparency in how they approach privacy, our own professional organization, which should set the standard, utilizes various trackers. On the homepage for the Association of Computing Machinery, acm.org, trackers for Google Analytics and AddThis can be found. On the popular Digital Library website with ACM, trackers from Twitter can also be found. As advocates for digital privacy, we encourage ACM to not use any trackers on their website. Besides, is there a real value gained to the organization from implementing these trackers?

Companies that focus on privacy as a core feature of their product is a positive direction, especially given the pervasiveness and ubiquity of these services in our lives. Both authors endorse this direction and advocate the use of products like DuckDuckGo. But, the research community needs to continue to ensure that these companies and their products or services match with what they advertise. Otherwise, their marketing of being privacy-focused companies is just marketing, and consumers can quickly lose trust in these companies. If that trust is lost, consumers may have more skepticism of similar services and may not support these alternatives. The stakes could not be higher as tracking has become more invasive and ubiquitous in the products we use. From our TVs to the devices we carry in our pockets, services are continually gathering various data points to create specific profiles so that advertisements can be more targeted. We need more privacy focused alternatives, but to support these alternatives, trust will be a key factor as it takes time to earn trust but it can be easily lost. These companies that provide alternatives services will need to ensure they are fully transparent with their users so that NDAs do not withhold trackers being used, logs are not shared without consent, and that privacy as a core feature of a product isn't used to increase revenue.

References

[1] DuckDuckGo, (2022). Your personal data is nobody's business. DuckDuckGo. https://duckduckgo.com/about.

[2] Heinzman, A., (2022). DuckDuckGo isn't as private as you thought. ReviewGeek. https://www.reviewgeek.com/118915/duckduckgo-isnt-as-private-as-you-thought/.

[3] Proton, (2022). Secure email that protects your privacy. Proton. https://proton.me/mail.

[4] Taylor, S. (2021). ProtonMail gives up logs on user, then scrubs website of no IP logging claims. Restore Privacy. https://restoreprivacy.com/protonmail-logs-users/.

[5] Yen, A., (2021). Important clarifications regarding arrest of climate activist. Proton. https://proton.me/blog/climate-activist-arrest.

[6] Proton, (2022). Transparency report. Proton. https://proton.me/legal/transparency.

[7] Germain, T., (2022). Apple is tracking you even when its own privacy settings say it's not, new research says. Gizmodo. https://gizmodo.com/apple-iphone-analytics-tracking-even-when-off-app-store-1849757558.

[8] Stokel-Walker, C., (2022). Apple is an ad company now. Wired. https://www.wired.com/story/apple-is-an-ad-company-now/.

Brian Krupp
Julia Gersey
Chambers University of Technology
Baldwin Wallace Univeristy
Berea, Ohio, USA
bkrupp@bw.edu