And their research observed what they termed a "targeted treatment of Apple's Safari web browser" where the advertising technology company Criteo (who mailed the letter I opened with) switched specifically to CNAME cloaking to bypass Safari's otherwise strong privacy protections.

And as for data leaks? Significant cookie data leaks were found on 95% of the sites that used CNAME tracking, all of which sent cookies containing private information such as full names, locations, email addresses, and even session authentication cookies to trackers of other domains without the user have any knowledge or control.

The entire presumption of cookies is that, bad and abuse-prone as they may be, at least they stay within the domain that set them. At least their content, whatever it might be — even if it's a user's actual name and real world identity, bad practice as that would be — at least it remains between those two parties. So while cookies can be used for tracking, the only data that is ever returned to a domain is something that that domain earlier sent. Thus, by definition it's not secret to that domain.

But now, thanks to the horrendous abuse of CNAMEs being used to deliberately confuse cookie domains, data is being sent with queries by user's web browsers to entities who never set that data in the first place. As the researchers noted, that data which should never be exposed to any third party, often contains information that tracking firms would die to have, and leverage. But now they don't have to. They just need to get websites to collude with them by adding a CNAME record to that domain's DNS.

The only good news here is that good old Gorhill's **uBlock Origin** add-on is at least partially effective at spotting and blocking accesses to these despicable subdomains:

Table 1. Overview of the analyzed CNAME-based trackers, based on the HTTP Archive dataset from October 2020.

Tracker	Detected # publishers	Est. total # publishers	Pricing (min. /mo)	requests to tracker is blocked by uBlock Origin Firefox	uBlock Origin Chrome	NextDNS CNAME blocklist
Pardot	5,993	21,759	$1,250	✔*	✔*	✖
Adobe Experience Cloud	2,612	9,029	$5,000†	✔	✔	✔
Act-On Software	1,041	2,533	$900	✔	✔	✖
Oracle Eloqua	304	3,743	$2,000†	✔	✖	✖
Eulerian	253	1,501	?	✔	✖	✔
Webtrekk	101	822	?	✔	✔	✔
Ingenious Technologies	41	-	?	✖	✖	✔
TraceDock	49	69	€49	✖	✖	✔
<intent>	14	124	?	✖	✖	✔
AT Internet	31	74	€355	✖	✖	✔
Criteo	16	13,082	?	✔	✖	✔
Keyade	12	86	?	✔	✖	✔
Wizaly	12	55	$2000†	✖	✖	✔

†: Pricing information does not originate from original source, but as reported in reviews of the product.
*: Requests made to the CNAME subdomain triggered by a third-party analytics script hosted on `pardot.com`; the blocklist prevents the analytics script from loading. If this script was loaded from the CNAME domain, it would not be blocked.