PrivacyMachine - creating random fingerprints to prevent web tracking

Introduction:

Today, web tracking[1] is not only achieved using cookies, but also makes use of far more advanced techniques such as fingerprinting[2]. The open source software PrivacyMachine provides a new concept for counteracting web tracking.

How is a fingerprint generated?
The most important properties of a fingerprint can be read by JavaScript and originally served the purpose of adapting a page to the browser used.
However, the combination of these properties, such as screen resolution or fonts installed in the operating system, is unique and makes it possible to recognise a computer on different pages.

The most elegant solution would be to read as little information as possible via JavaScript and for this to be standardised. But the finances necessary for developing a competitive modern browser mean this is only possible for large companies.

Previous approaches to counteracting web tracking involved attempting to create a large group of users who have the same fingerprint when surfing the web. This means it is no longer possible to identify individual users in the group.
A well-developed example of this approach is the TOR browser.
The following pages calculate how unique a fingerprint is:
https://panopticlick.eff.org
https://amiunique.org

These pages clearly show that it is almost impossible to be in a group of any relevant size without taking drastic measures such as turning off JavaScript.
Most browser setups are unique.

Implementing countermeasures, which are usually achieved by installing several browser plug-ins, have two effects:

- The usability of pages is drastically reduced, because numerous individual options for a page need to be manually unblocked in order for it to work (example: NoScript)
- Each installed plug-in decreases anonymity, because the list of installed plug-ins is also part of the fingerprint.

1 „Web tracking“ refers to the recognition of users on different web pages.
2 A „fingerprint“ consists of all the properties that make a computer unique.

Why is the PrivacyMachine concept different?

The PrivacyMachine looks like a normal browser; the difference is that a virtual machine is running behind each tab, which shows the content of a standard browser. Every virtual machine is given its own IP address via VPN or TOR.
The advantage is that the machine is reset to a snapshot when the tab is closed → all types of cookies, such as Flash cookies or browser local storage, are deleted.
Furthermore, the fingerprint is changed by altering the properties of the operating system and installed software. These properties make up most of the fingerprint, which is read by the browser using JavaScript and sent to web tracker domains.

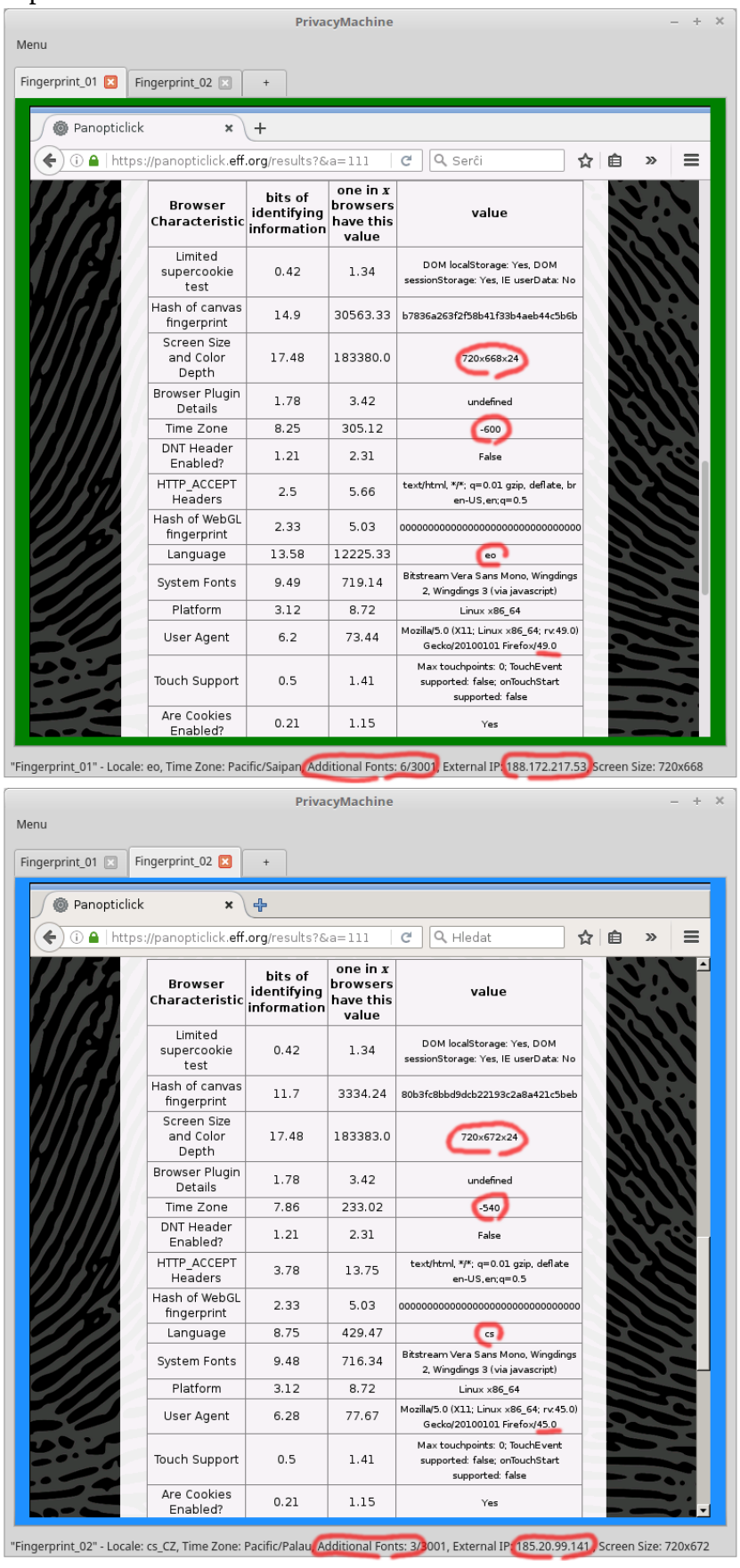
Every time a tab is opened, a new unique fingerprint is created.
The user can surf using two different fingerprints in parallel.

Can a user be recognised precisely because their fingerprint is unique?

Yes, if there is only one user. However, it would not make financial sense for a tracking provider to implement the recognition of one individual user.

If a group of, for example, 20 people use the PrivacyMachine, it is not possible to differentiate between individual users. The averaged personal profile either would not make sense – because sex and age change – or the combined profile would be something as general as readers of a print medium → **the users are then only shown non-personalised advertisements and the creation of comprehensive personal profiles is prevented.**

This screenshot from https://panopticlick.eff.org shows two fingerprints in two VM masks (virtual machines) that are open at the same time.



Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.42	1.34	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	14.9	30563.33	b7836a263f2f58b41f33b4aeb44c5b6b
Screen Size and Color Depth	17.48	183380.0	720x668x24
Browser Plugin Details	1.78	3.42	undefined
Time Zone	8.25	305.12	-600
DNT Header Enabled?	1.21	2.31	False
HTTP_ACCEPT Headers	2.5	5.66	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5
Hash of WebGL fingerprint	2.33	5.03	00000000000000000000000000000000
Language	13.58	12225.33	eo
System Fonts	9.49	719.14	Bitstream Vera Sans Mono, Wingdings 2, Wingdings 3 (via javascript)
Platform	3.12	8.72	Linux x86_64
User Agent	6.2	73.44	Mozilla/5.0 (X11; Linux x86_64; rv:49.0) Gecko/20100101 Firefox/49.0
Touch Support	0.5	1.41	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.21	1.15	Yes

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.42	1.34	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	11.7	3334.24	80b3fc8bbd9dcb22193c2a8a421c5beb
Screen Size and Color Depth	17.48	183383.0	720x672x24
Browser Plugin Details	1.78	3.42	undefined
Time Zone	7.86	233.02	-540
DNT Header Enabled?	1.21	2.31	False
HTTP_ACCEPT Headers	3.78	13.75	text/html, */*; q=0.01 gzip, deflate en-US,en;q=0.5
Hash of WebGL fingerprint	2.33	5.03	00000000000000000000000000000000
Language	8.75	429.47	cs
System Fonts	9.48	716.34	Bitstream Vera Sans Mono, Wingdings 2, Wingdings 3 (via javascript)
Platform	3.12	8.72	Linux x86_64
User Agent	6.28	77.67	Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Touch Support	0.5	1.41	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.21	1.15	Yes

Authors: Bernhard Zach, Olaf Pichler, Alexander Leopold
contact@privacymachine.eu
OpenPGP-Fingerprint: 0C93 F15A 0ECA D404 413B 5B34 C6DE E513 0119 B175