NOT SIMILAR TO COOKIES: DEVICE AND BROWSER FINGERPRINTING AS SENSITIVE PERSONAL DATA

Mark Nottingham

I Introduction

Browser and device fingerprinting are especially pernicious methods of online tracking, but most legal responses have not distinguished them from a more well-known mechanism, cookies, despite having a reputation as being 'creepy'.[1] I contend that they deserve separate consideration, owing to the distinct privacy challenges they present.

In this paper I briefly explain what fingerprinting is, summarise how online trackers use it, and explore the privacy issues raised, especially as compared to cookies. I evaluate the current constraints on fingerprinting using Lessig's norms/market/architecture/law framework of regulation modalities. I then discuss why fingerprints should not only be considered as distinct from cookies, but should also be considered as sensitive data, deserving of a distinct legal response. Finally, I outline potential legal responses to fingerprinting, exploring their tradeoffs.

II What is fingerprinting?

In this paper, fingerprinting refers to two related techniques — *browser fingerprinting* and *device fingerprinting*.

Browser fingerprinting is 'a method of web browser identification based on information provided by each web browser, such as the screen size, the list of installed plugins, system languages, and other [mechanisms].'[2]

Device fingerprinting is the use of similar methods to identify the device being used — e.g., the desktop, laptop, or mobile computer. This technique can be successful even when different software is used to access a service (e.g., after switching Web browsers).[3]

---

[1] See, eg, Adam Tanner, 'The Web Cookie Is Dying. Here's The Creepier Technology That Comes Next', *Forbes* (online, 17 June 2013) <https://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/>.

[2] Peter Hraska, 'Browser Fingerprinting' (Master's Thesis, Comenius University, 2018).

[3] Yinzhi Cao, Song Li, and Erik Wijmans, '(Cross-)Browser Fingerprinting Via OS and Hardware Level Features' [2017] *Proceedings of the Network and Distributed System Security Symposium.*

First brought to wide attention over a decade ago by Peter Eckersley,[4] fingerprinting is not dependent upon the user's IP address, nor upon something being stored on their computer; rather, it uses the combination of slight differences in the computer and client software (in the case of browser fingerprinting, the Web browser) and their configuration to re-identify it (and thus its user) later.

A fingerprint's ability to identify a device or browser uniquely is measured in *bits of entropy:* each potential difference from other devices or browsers "leaks" some amount of entropy. Eckersley explains:

> Intuitively you can think of entropy being generalisation of the number of different possibilities there are for a random variable: if there are two possibilities, there is 1 bit of entropy; if there are four possibilities, there are 2 bits of entropy, etc. Adding one more bit of entropy doubles the number of possibilities.[5]

Because there are approximately 8 billion people, it's possible to assign a unique identifier to every person using 33 bits of entropy (as two to the power of 33 is about 8.5 billion). Typically, a Web site creates a fingerprint by combining several such sources of entropy. If the cumulative bits of entropy are sufficiently unique, the fingerprint can thus be used to identify the associated user.[6]

Those sources of fingerprinting entropy include information that the client emits without solicitation (e.g., HTTP request header fields) and that obtained by manipulating its provided interfaces (e.g., in JavaScript APIs). The former is known as *passive fingerprinting* because its use is not detectable by examining how the client interacts with the service; the latter is *active fingerprinting*, and in theory can be detected by observing how a service uses those interfaces.[7]

---

[4] Peter Eckersley, 'How Unique Is Your Web Browser?' in Mikhail J Atallah and Nicholas J Hopper (eds), *Privacy Enhancing Technologies* (Springer Berlin Heidelberg, 2010) 1.

[5] Peter Eckersley, 'A Primer on Information Theory and Privacy' (Blog Post, 26 January 2010). <https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy>.

[6] Eckersley (n 4).

[7] Nick Doty, 'Mitigating Browser Fingerprinting in Web Specifications' (W3C Editor's Draft, 2020) § 3 <https://w3c.github.io/fingerprinting-guidance>.

For example, an aspiring fingerprinter might observe that someone is using a particular build of the Safari Web browser by examining the User-Agent request header it sends. If a given value is only used by one in 76.38 browsers, that conveys 6.26 bits of entropy. If the time zone it is configured to use (as exposed by a JavaScript API) is shared by only one in 89.65 other browsers, that conveys an additional 6.49 bits of entropy. If the list of installed fonts is examined (again using JavaScript), that might add even more entropy.[8] Note that this is a simplistic example: commercial products using fingerprinting boast of using over 200 sources of entropy to assure uniqueness.[9]

Importantly, a fingerprint persists even when the user takes active steps to frustrate tracking; e.g., clearing cookies, changing network address through use of a VPN, or using the browser's so-called 'private mode.'[10] This property makes the moniker that Eckersley chose in 2010 especially apt; just as it is difficult to change a physical fingerprint, it is also difficult to change a browser or device fingerprint.

A fingerprint changes over time. For example, updates to client software and the operating system that hosts it might cause a fingerprint to change, since they often rely on specific aspects of both.[11] Or, a fingerprint might change because the user has installed, uninstalled or upgraded browser extensions or system fonts. Another factor causing flux is what can be seen as an escalation between fingerprinting and anti-fingerprinting techniques; in particular, as Web browsers have become more sophisticated in preventing fingerprinting, new fingerprinting techniques have been discovered.

Despite their shifting nature, browser fingerprints are stable enough to track up to 94.5% of users for a period of up to 11.9 weeks, according to Pugliese et al.[12] When used in concert with other tracking mechanisms like cookies, so-called 'super-cookies', IP address information[13] and geolocation, they can re-identify the browser or device in question even when the user clears cookies, changes networks, and changes location.

---

[8] 'Cover Your Tracks' (Web Page) <https://coveryourtracks.eff.org>.

[9] See, eg, 'The Evolution of Hi-Def Fingerprinting in Bot Mitigation' (Web Page) <https://www.imperva.com/blog/the-evolution-of-hi-def-fingerprinting-in-bot-mitigation/>.

[10] Sakchan Luangmaneerote, 'Defences against Browser Fingerprinting Techniques' (Thesis, University of Southampton, 1 November 2018) 2.

[11] Song Li and Yinzhi Cao, 'Who Touched My Browser Fingerprint?: A Large-Scale Measurement Study and Classification of Fingerprint Dynamics' [2020] *ACM Internet Measurement Conference* 370.

[12] Gaston Pugliese et al, 'Long-Term Observation on Browser Fingerprinting: Users' Trackability and Perspective' [2020] (2) *Proceedings on Privacy Enhancing Technologies* 558.

[13] Vikas Mishra et al, 'Don't Count Me Out: On the Relevance of IP Address in the Tracking Ecosystem' [2020] *Proceedings of the World Wide Web Conference* 808.

See <https://amiunique.org/> for a demonstration of browser fingerprinting, and visit <https://www.ipqualityscore.com/device-fingerprinting> with two browsers on the same device for a demonstration of cross-browser device fingerprinting.

III Uses of fingerprinting

Web sites can use the identifier provided by a fingerprint for a variety of purposes.

A *Fraud prevention*

Automated clients (also known as *bots*) are a significant problem for online services, because they are often malicious. For example, a bot might be used to overwhelm a site with requests that consume its resources in a Distributed Denial-of-Service attack,[14] find and exploit vulnerabilities due to outdated or buggy software,[15] register large numbers of fake accounts for illegitimate purposes,[16] guess passwords of existing accounts (known as credential stuffing),[17] or to scrape pricing and other proprietary information.[18]

This has led to the development of a diverse landscape of anti-bot solutions, both commercial and Open Source.[19] Fingerprinting is commonly used in these products, including those from reputable companies such as Microsoft[20] and Oracle.[21]

---

[14] Karanpreet Singh, Paramvir Singh and Krishan Kumar, 'Application Layer HTTP-GET Flood DDoS Attacks: Research Landscape and Challenges' (2017) 65 *Computers and Security* 344.

[15] See, e.g., Jai Vijayan, 'NSA Warns of Exploits Targeting Recently Disclosed VMWare Vulnerability' (7 December 2020) *DARKReading* <https://www.darkreading.com/threat-intelligence/nsa-warns-of-exploits-targeting-recently-disclosed-vmware-vulnerability/d/d-id/1339632>.

[16] See, eg., Zi Chu et al, 'Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?' (2012) 9(6) *IEEE Transactions on Dependable and Secure Computing* 811.

[17] Steven Rees-Pullman, 'Is Credential Stuffing the New Phishing?' [2020] (7) *Computer Fraud and Security* 16.

[18] Rizwan Ur Rahman and Deepak Singh Tomar, 'Threats of Price Scraping on E-Commerce Websites: Attack Model and Its Detection Using Neural Network' [2020] *Journal of Computer Virology and Hacking Techniques*.

[19] Babak Amin Azad et al, 'Web Runner 2049: Evaluating Third-Party Anti-Bot Services' [2020] *17th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*.

[20] 'DFP and Mobile Device fingerprinting', *Microsoft Support* (Web Page, 23 June 2020) <https://support.microsoft.com/en-au/help/4569098/mobile-device-fingerprinting>.

[21] 'Device Fingerprinting', *Oracle Help Center* (Web Page) <https://docs.oracle.com/cd/E27559_01/admin.1112/e60559/finger.htm#AAMAD6186>.

Tracking a client with a fingerprint is advantageous for fraud prevention because it allows a site to identify a badly behaved client and reject future requests from it.[22] Likewise, fingerprinting allows a service to be more confident in the identity of legitimate clients, and can be used to determine whether additional security measures are needed to authenticate the user.[23]

However, fingerprinting's effectiveness for this purpose has recently been called into question, as attackers have adapted to its use by appropriating legitimate fingerprints to bypass such measures, with an illicit marketplace in stolen fingerprints recently forming.[24]

B *Audience Measurement*

Sometimes referred to as Web analytics, the 'capability to measure interactions of website visitors [provides] previously unknown levels of insight into the effectiveness of marketing communications'.[25] Audience measurement allows sites to optimise functionality, understand past performance, improve conversions from marketing campaigns, test different options to find the optimal one (referred to as *A/B testing*), inform site redesigns, predict how future campaigns will perform, and budget for upcoming business objectives.[26]

As with fraud prevention, fingerprinting is useful for audience measurement because it persists even when cookies are disabled, blocked, or cleared. As a result, it is used by Web analytics frameworks as a way to identify visitors to a site.[27]

---

[22] See, eg, Tamas Kadar, 'Browser Fingerprinting – Good for Fraud Detection, But Is It Enough?', *Seon* (Web Page) <https://seon.io/resources/browser-fingerprinting-good-for-fraud-detection-but-is-it-enough/>.

[23] See, eg, Martin Gallo, 'Why Browser Fingerprinting is Creating Challenges for Identity Security', *SecureAuth* (Web Page) <https://www.secureauth.com/blog/why-browser-fingerprinting-is-creating-challenges-for-identity-security/>.

[24] Ariel Ainhoren, 'Digital Browser Identities: The Hottest New Black Market Good', (Research Report, IntSights, 2019) <https://intsights.com/resources/research-report-digital-browser-identities>.

[25] Dave Chaffey and Mark Patron, 'From Web Analytics to Digital Marketing Optimization: Increasing the Commercial Value of Digital Analytics' (2012) 14(1) *Journal of Direct, Data and Digital Marketing Practice* 30.

[26] Ibid 33.

[27] See, eg, 'How Does Matomo Detect Unique and Returning Visitors?', *Matomo* (Web Page) <https://matomo.org/faq/general/faq_21418/>.

C *Online Behavioural Advertising*

The FTC defines Online Behavioural Advertising (OBA) as 'the tracking of consumers' online activities in order to deliver tailored advertising.'[28] Similarly, the Article 29 Working Party explains that behavioural advertising 'entails the tracking of users when they surf the Internet and the building of profiles over time, which are later used to provide them with advertising matching their interests.'[29]

While those profiles are most widely understood to be built using cookies, there is evidence that fingerprinting is commonly used for OBA, despite difficulties measuring it and a reluctance to discuss it amongst many in the industry. A February 2020 IAB paper makes it clear that '[c]ookies and fingerprints are at the heart of the buying and selling of advertising.'[30] Similarly, advertising industry press characterises the technique as 'a widely used practice.'[31]

Fingerprints can serve several functions in OBA, including:

- Completely replacing cookies as a tracking mechanism. This gives the tracker more control (because there are no cookies that the user is able to delete or block), and makes tracking less visible.
- Augmenting cookies, by re-establishing tracking when the user removes the tracking cookie.
- Tracking selectively when cookies are not available; e.g., when they are disabled, blocked by a browser extension, or by a 'private browsing' mode.[32]
- Tracking across devices; e.g., when watching a movie on an Internet-connected TV and using your phone at the same time.[33]

---

[28] *Self-Regulatory Principles for Online Behavioral Advertising* (FTC Staff Reports, February 2009).

[29] *Opinion 2/2010 on Online Behavioral Advertising* (Advisory Opinion) (Article 29 Data Protection Working Party, WP 171, 22 June 2010) 3.

[30] John Deighton and Leora Kornfeld, 'The Socioeconomic Impact of Internet Tracking' (Discussion Paper, Internet Advertising Bureau, February 2020) 13 <https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf>.

[31] Ronan Shields, 'What Google's War on Fingerprinting Means for Marketers' (20 May 2019) *AdWeek* <https://www.adweek.com/programmatic/what-googles-war-on-fingerprinting-means-for-marketers/>.

[32] Pugliese et al (n 12) 571.

[33] Cao, Li, and Wijmans (n 3).

The economic value of OBA is often disputed; while the market is large, the actual returns to advertisers are difficult to measure, due to selection bias.[34] Nevertheless, there is some evidence that privacy regulation does have an effect on its outcomes.[35]

D *Data-oriented uses*

Although fingerprints are described in terms of bits of entropy, it is a secondary use of the data the fingerprint is based upon; in each case, the source of entropy has another primary use (typically, customising the content to the capabilities of the device in question or the preferences of the user).

This information can be used for a variety of purposes, at turns benign and malignant. It can be used to provide useful functionality to the end user, and it can directly leak sensitive information from them (e.g., exposing their affinities based upon the browser extensions installed).[36]

As a result, it's not possible for clients to simply stop sending the information that's used for fingerprinting; instead, its utility is weighed against the risk of fingerprinting as well as other privacy and security issues on a case-by-case basis.[37]

E *How prevalent is use of fingerprinting?*

Because the difference in these uses of fingerprinting are largely of intent, it is difficult to measure their relative prevalence on the Internet. Likewise, the absolute prevalence of fingerprinting for any purpose is also difficult to measure, because active fingerprinting can look like legitimate interaction, and passive fingerprinting on its own is not detectable.

Nevertheless, a recent study by Al-Fannah et al. shows that 68.8% of the 10,000 most popular Web sites are potentially fingerprinting, as judged by the information sent to them upon interacting with their home pages.[38] Of those sites, 84.5% send that data only to third parties.[39]

---

[34] Randall A Lewis and Justin M Rao, 'The Unfavorable Economics of Measuring the Returns to Advertising' (2015) 130(4) *Quarterly Journal of Economics* 1941.

[35] Avi Goldfarb and Catherine E Tucker, 'Privacy Regulation and Online Advertising' (2011) 57(1) *Management Science* 57.

[36] Soroush Karami et al, 'Carnus: Exploring the Privacy Threats of Browser Extension Fingerprinting' [2020] (February) *Network and Distributed Systems Security Symposium*.

[37] See below s V(C).

[38] Nasser Mohammed Al-Fannah, Wanpeng Li and Chris J Mitchell, *Beyond Cookie Monster Amnesia: Real World Persistent Online Tracking*, vol 1 (Springer, 2018) 489.

[39] Ibid.

However, it must be noted that this is *potential* fingerprinting; the information could be collected for other purposes, with no fingerprint being kept. Another study that looked for more positive evidence of fingerprinting (with a corresponding risk of under-counting) found that about 850 of the top 10,000 European sites use it.[40]

IV Privacy issues raised by fingerprinting

Online tracking raises significant privacy issues regardless of the specific method used because it facilitates the creation of a profile of a person's activity across the online sphere. Schwartz's observation in 1999 that 'Internet behavior generates more finely grained personal data than Real Space activities such as the use of a credit card'[41] has become matter-of-fact, with online tracking now being considered 'ubiquitous' and 'impossible to avoid.'[42]

A common objection to these privacy concerns is that advertisers are only interested in targeting certain classes of people, rather than individuals. However, there are a number of situations where targeting data can be tied to an individual, thereby qualifying it as personal data.[43] The underlying intent does not matter; it is the collection and processing of the data that raise the concerns on their own.

The specific privacy harms associated with online tracking can be categorised using Ohm's framework of ancient, traditional and modern harms.[44] Because of its ubiquity, all three categories of harm are possible.

For example, knowing that someone shops for, searches for, or views things that they might be ashamed of or otherwise reluctant to reveal could facilitate the ancient harms of emotional distress, harassment and blackmail, depending on how the information is used. A comprehensive profile of one's activity also might be an aid to identity theft and stalking.

Likewise, such a profile might lead to the traditional dignitary harms of humiliation, abasement, or ostracism if it became available to one's friends, work colleagues or neighbours.

---

[40] Mohammadreza Ashouri, 'A Large-Scale Analysis of Browser Fingerprinting via Chrome Instrumentation' Research Report, Universität Potsdam, 23 July 2019).

[41] Paul M Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52(6) *Vanderbilt Law Review* 1609.

[42] Hassan Metwalley et al, 'The Online Tracking Horde: A View from Passive Measurements' (2015) 9053 *International Federation for Information Processing* 111.

[43] Frederik J Zuiderveen Borgesius, 'Singling out People without Knowing Their Names - Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation' (2016) 32(2) *Computer Law and Security Review* 256.

[44] Paul Ohm, 'Sensitive Information' [2014] (88) *S. Cal. L. Rev.* 1161.

Finally, the modern harm of losing control over one's information is perhaps the most likely when third parties are capable of tracking what one does online, a space that is increasingly necessary for modern life.

There is active and ongoing debate about how to balance these potential harms against the interests of Web sites, especially when the services they provide to users are funded by Online Behavioural Advertising. While fingerprinting inherits these potential harms, it magnifies their likelihood and frustrates mitigations in two distinct ways — especially in comparison with a more well-understood tracking mechanism, HTTP cookies.

A *Lack of control*

If privacy is considered to be control over personal data, perhaps the most concerning aspect of fingerprinting is users' inability to control it; one cannot reliably change their browser's or device's fingerprint through positive actions, and it is difficult if not impossible to prevent a fingerprint from being collected.

The lack of control afforded to users is not passive; fingerprinting technology actively resists attempts to control tracking. The availability of increasingly sophisticated techniques means that a determined tracker can re-identify a user despite clearing cookies and other browser state, despite using a different browser, and even despite using a Virtual Machine to obscure the underlying hardware.[45]

In contrast, cookies defined to only operate within a certain scope,[46] can be selectively blocked (e.g., by a browser extension), or completely removed ('clearing cookies') or temporarily removed ('privacy mode') through affordances in the browser. Users can also completely disable the cookie function in their browser.

Many users take advantage of these mechanisms to control their privacy when using the Internet. For example, in 2013, Rainie et al. found that 64% of adult Internet users in the US surveyed clear cookies and browser history to avoid being observed — by far the most popular strategy captured by the survey.[47] In 2018, Boerman et al. find that people 'most often delete cookies and browser history or decline cookies to protect their online privacy.'[48]

---

[45] Yossef Oren et al, 'The Spy in the Sandbox: Practical Cache Attacks in JavaScript and Their Implications' October 20 *Proceedings of the ACM Conference on Computer and Communications Security* 1406.

[46] Adam Barth, 'HTTP State Management Mechanism' (IETF Proposed Standard, RFC 6265, April 2011) 10.

[47] Lee Rainie et al, *Anonymity, Privacy, and Security Online* (Report, Pew Research Center, 5 September 2013) <http://www.pewinternet.org/Reports/2013/Anonymity-online.aspx>.

[48] Sophie C Boerman, Sanne Kruikemeier and Frederik J Zuiderveen Borgesius, 'Blocking Ads and Deleting Cookies: A Longitudinal Study Examining Online Privacy Protection Behavior' [2018] *American Academy of Advertising Conference Proceedings* 85.

Furthermore, GlobalWebIndex reports that more than 4 in 10 Internet users globally employed an ad-blocking browser extension in March 2018; 1 in 4 of say that a primary motivation for ad-blocking is privacy.[49]

B *Lack of transparency*

The lack of visibility into fingerprinting is also troubling. Even technical experts can easily confuse it with legitimate processing; passive fingerprinting is difficult (if not impossible) to detect.[50] The exact techniques that are used to create a fingerprint change over time, as well as from site to site.[51]

As a result, whether fingerprinting is taking place is not visible to users; they are required to trust the assertions of the parties they communicate with as to whether fingerprinting is taking place, and how fingerprints are reused in the future. This creates a moral hazard for online trackers.

Because of this lack of transparency, it is also difficult for users to verify that a change they make in an effort to avoid tracking by fingerprint is effective. Likewise, research into the prevalence of fingerprinting can only use indirect measurements that are prone to under- or over-estimation, leading to a lack of visibility into the use and nature of fingerprinting overall.

Furthermore, it is not possible to know when a fingerprint is reused for an unauthorised purpose — whether the fingerprint was collected legitimately or illegitimately (as evidenced by the emergence of an underground marketplace for fingerprints).[52]

In contrast, cookies are visible and legible to the end user; browsers often allow inspection of individual cookie values, and their operation is explicit and uniform, because it is defined by a technical standard. Thus, it is possible to know when a cookie is lodged in the user's browser as well as when they are collected by a server, and researchers can leverage that knowledge to understand how they are used.

V Current regulation of fingerprinting

One way to understand the current regulation of fingerprinting is through Lessig's lens of four modalities of regulation: norms, market, architecture, and law.[53]

---

[49] Olivia Valentine, 'Privacy Concerns Lead to Ad-Blocking' (Blog Entry, 5 April 2018) <https://blog.globalwebindex.com/chart-of-the-day/privacy-concerns-ad-blocking/>.

[50] Doty (n 7) § 6.3.

[51] Pugliese (n 12).

[52] Ainhoren (n 24).

[53] Lawrence Lessig, *Code version 2.0* (Basic Books, 2006) ch 7.

A *Regulation by norm*

Overall, norms around online tracking have proven hard to develop, as seen in the failure of the Do Not Track effort, which started as an attempt at industry self-regulation (thereby being a form of regulation by norm enabled by an architectural mechanism, *not* regulation by architecture).[54]

There is little effective regulation of fingerprinting by norms, in part because this tracking technique is not widely understood by the public. McDonald and Cranor note that based upon their lab study, fingerprinting is 'invisible to users to the point we would be wasting our time and theirs to ask…'[55]

Nevertheless, there have been some attempts to establish explicit norms around fingerprinting; for example, the W3C Technical Architecture Group has characterised fingerprinting as a form of 'unsanctioned tracking' that can 'undermine user trust in the Web itself'.[56] The Internet Architecture Board further characterises it as a potential vulnerability in protocol design.[57]

The Electronic Freedom Foundation[58] and Center for Democracy and Technology[59] have created educational and advocacy materials that explain fingerprinting in the context of online privacy. The EFF also created the Panopticlick tool[60] to illustrate how fingerprinting works, and how effective it is.

These efforts are of limited effect because it's not possible to see how a service is fingerprinting you using available tools; while there is research into the prevalence of fingerprinting, determining its use currently requires after-the-fact analysis. The hidden and amorphous nature of fingerprinting makes it difficult to form norms around it in the wider public, as has happened for cookies.

---

[54] Irene Kamara and Eleni Kosta, 'Do Not Track Initiatives: Regaining the Lost User Control' (2016) 6(4) *International Data Privacy Law* 276.

[55] Aleecia M McDonald and Lorrie Faith Cranor, 'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising' [2010] *Telecommunications Policy Research Conference*.

[56] Mark Nottingham, 'Unsanctioned Web Tracking' (W3C TAG Finding, 17 July 2015) <https://www.w3.org/2001/tag/doc/unsanctioned-tracking/>.

[57] Alissa Cooper et al, 'Privacy Considerations for Internet Protocols' (IAB Informational RFC, July 2013) <https://tools.ietf.org/html/rfc6973>.

[58] 'What is Fingerprinting', *Surveillance Self-Defence* (Web Page, 14 July 2020) <https://ssd.eff.org/en/module/what-fingerprinting>.

[59] Greg Norcie, 'Unsanctioned Web Tracking is Harmful', *Center for Democracy and Technology* (Web Page, 31 July 2015) <https://cdt.org/insights/unsanctioned-web-tracking-is-harmful/>.

[60] 'Panopticlick 3.0' (Web page) <https://panopticlick.eff.org/>.

At the same time, it appears that norms are emerging in specific industries that condone the use of fingerprinting for various purposes. In particular, fingerprinting appears to be well on its way to being established as a norm for the purpose of fraud prevention.[61]

The advertising technology industry is less forthcoming about how it uses fingerprinting, likely because it is sensitive to negative consumer reception of the technique. In 2016, Englehardt and Narayanan asserted that there is a 'self-regulatory norm regarding acceptable uses of fingerprinting',[62] but none is readily evident in the communications of its peak body, the Internet Advertising Bureau.

The conflict between these user-focused and industry-focused needs is difficult to resolve within the framework of norms. In many ways this debate mirrors that surrounding the use of cookies — except that fingerprinting is an ad hoc tracking practice that is less visible and more difficult to evade.

B *Regulation by the market*

Market-based regulation of online tracking is notoriously difficult. As Jakobi et al. observe, '[t]he information asymmetry between operators of trackers and end-users is so extensive that the market… fails to function.'[63]

This asymmetry is more pronounced in the case of tracking by fingerprinting, because there is no direct information regarding fingerprinting available to the end user, who at the same time is pulled by other aspects of the market (shopping, being entertained, getting their work done) to accept tracking as a fact of life, since a substantial portion of the online world is advertising-funded, and behavioural tracking is part of that.

Furthermore, the act of fingerprinting is not expensive; there are Open Source projects that provide fingerprinting libraries for free,[64] as well as a variety of commercial services.[65]

---

[61] See above s III(A).

[62] Steven Englehardt and Arvind Narayanan, 'Online Tracking: A 1-Million-Site Measurement and Analysis' [2016] *Proceedings of the ACM Conference on Computer and Communications Security* 1398.

[63] Timo Jakobi et al, 'Web Tracking under the New Data Protection Law: Design Potentials at the Intersection of Jurisprudence and HCI' (2020) 19(1) *I-Com* 31.

[64] See, eg, 'FingerprintJS' (Web Page) <https://github.com/fingerprintjs/fingerprintjs>.

[65] See above s III(A).

Privacy-conscious users might identify use of fingerprinting through a process of elimination; for example, if you see what appears to be targeted advertising in a Web browser despite clearing cookies and using private browsing, there are few ways left for tracking to have occurred outside of fingerprinting. This might lead to a limited form of regulation in privacy-sensitive markets; for example, DuckDuckGo was quick to respond to allegations of tracking by browser fingerprinting in 2019.[66]

C *Regulation by architecture*

Much discussion and activity to date has focused on how fingerprinting can be mitigated by changing architecture — specifically, the behaviour of Web browsers.

Because of its security and privacy focus, Tor Browser was one of the first browsers to focus on fingerprinting mitigation,[67] and Firefox subsequently adopted those modifications.[68]

More recently, browser vendors have taken significant (albeit often uncoordinated) steps to reduce cross-site tracking overall, because of its perceived impact on end user privacy. While much of these efforts focus on constraining the use of cookies (e.g., Apple Safari's Intelligent Tracking Prevention;[69] Mozilla Firefox's Enhanced Tracking Protection,[70] and Google Chrome's Privacy Sandbox),[71] mitigating fingerprinting is seen as a necessary complement to those efforts because otherwise those with a strong incentive to track users online would simply change from using cookies to using fingerprinting.

---

[66] Natasha Lomas and Zack Whittaker, 'DuckDuckGo: No, We're Not Using Browser Fingerprinting to Track You' (8 January 2019) *TechCrunch* <https://techcrunch.com/2019/01/07/duckduckgo-browser-fingerprinting/>.

[67] Mike Perry et al, 'The Design and Implementation of the Tor Browser', *Tor* (Web Page, 15 June 2018) <https://2019.www.torproject.org/projects/torbrowser/design/#fingerprinting-linkability>.

[68] 'Security/Tor Uplift', *mozilla wiki* (Web Page, 18 July 2019) <https://wiki.mozilla.org/Security/Tor_Uplift>.

[69] John Wilander, 'Intelligent Tracking Prevention 2.3', *WebKit* (Web Page, 23 September 2019) <https://webkit.org/blog/9521/intelligent-tracking-prevention-2-3/>.

[70] 'Enhanced Tracking Protection in Firefox for Desktop', *mozilla Support* (Web Page) <https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop>.

[71] 'The Privacy Sandbox', *The Chromium Projects* (Web Page) <https://www.chromium.org/Home/chromium-privacy/privacy-sandbox>.

As a result, there have been corresponding efforts to limit opportunities for fingerprinting by the major browser engines (Gecko,[72] WebKit,[73] and Chromium),[74] as well as many browsers using them (e.g., Brave).[75]

Currently, these efforts use several techniques to counter fingerprinting, including:

- **Homogenisation of browsers** so that they cannot be distinguished from each other. For example, there have been proposals to either remove the User-Agent request header field, or to fix its value regardless of the browser producing it, to remove this aid to fingerprinting.[76] However, differences between browsers only represent some sources of entropy, and some differences are so subtle that they cannot be practically removed.
- **Reduction of information quality**. For example, in response to the fingerprinting risks in the Ambient Light Sensor API exposed by Olejnik,[77] Chrome chose to round its output, to reduce the amount of entropy exposed. This is a direct tradeoff between functionality and privacy, and may be difficult to balance universally.
- **Randomisation of values** that have fingerprinting risk. This is an alternative to homogenisation; rather than making everything look the same, it makes every browsing session look different, by seeding different values and behaviours with randomness. Brave has adapted this technique.[78] However, this requires knowledge of the sources of entropy that the fingerprinter is using, and has some usability challenges.[79]

---

[72] 'Firefox's Protection Against Fingerprinting', *mozilla Support* (Web Page) <https://support.mozilla.org/en-US/kb/firefox-protection-against-fingerprinting>.

[73] 'Safari Privacy Overview', *Appl*e (Web Page, November 2019) <https://www.apple.com/safari/docs/Safari_White_Paper_Nov_2019.pdf>.

[74] Brad Lassey, 'Combatting Fingerprinting with a Privacy Budget' (Web Page, 28 August 2019) <https://github.com/bslassey/privacy-budget>.

[75] Peter Snyder, 'Fingerprinting Protections', *Brave Browser* (Web Page, 27 August 2020) <https://github.com/brave/brave-browser/wiki/Fingerprinting-Protections>.

[76] Pierre Laperdrix et al, 'Browser Fingerprinting: A Survey' (2020) 14(2) *ACM Trans. Web*. s 4.2.

[77] Lukasz Olejnik, 'Shedding Light on Web Privacy Impact Assessment: A Case Study of the Ambient Light Sensor API' (2020) *IEEE European Symposium on Security and Privacy Workshops* 310.

[78] Snyder (n 75).

[79] Frederic Besson, Nataliia Bielova and Thomas Jenson, 'Browser Randomisation against Fingerprinting: A Quantitative Information Flow Approach' [2014] *NordSec 2014: Secure IT Systems* 181.

- **Converting passive into active fingerprinting**. For example, the Client Hints specification requires a server to solicit information from the browser before it is offered in requests.[80] Active fingerprinting is at least theoretically detectable, but as discussed previously, measuring it still presents significant problems.
- **Managing the pool of available entropy**. For example, Chrome's Privacy Sandbox proposes that a site has a 'privacy budget' that only allows access to a capped amount of entropy; if it uses too many features, that is assumed to be evidence of fingerprinting, and access to those features will be denied.[81] This approach is still unproven, and some potential flaws have already been identified.[82]

Concurrently, there has been growing concern about fingerprinting 'surface area' (i.e., additional bits of entropy) in new Web specifications. While there is considerable pressure to add new APIs to keep the Web platform competitive with others (e.g., mobile phone app platforms), it is now widely agreed that a new feature that exposes more entropy that can be used for passive fingerprinting of browsers should be avoided. Furthermore, when exposure of entropy through active fingerprinting cannot be avoided, a new feature is required to justify this.[83]

Even with such a variety of activity to mitigate fingerprinting through architectural changes in standards and in browser implementations, there is widespread pessimism about long-term success in doing so among those engaging in the work. Al-Fannah et al remark that 'preventing browser fingerprinting is likely to be impossible.'[84]

This pessimism has a number of potential sources. First, because Web browsers have a strong incentive to be compatible with as much existing Web content as possible (if they are not compatible, they are vulnerable to being replaced by a competitor); it effectively requires them to implement the complete set of APIs and capabilities that Web browsers have historically supported. Taken as a whole, these capabilities have broad potential for fingerprinting, but they are unlikely to be deprecated and they are difficult to modify to improve privacy without affecting functionality on Web sites that use them.

---

[80] Ilya Grigorik and Yoav Weiss, 'HTTP Client Hints' (IETF Internet-Draft, 3 July 2020) <https://datatracker.ietf.org/doc/draft-ietf-httpbis-client-hints/>.

[81] Lassey (n 74).

[82] See, eg, Peter Snyder, 'Brave, Fingerprinting and Privacy Budgets', *Brave* (Web Page, 6 November 2019) <https://brave.com/brave-fingerprinting-and-privacy-budgets/>.

[83] Doty (n 7).

[84] Nasser Mohammed Al-Fannah and Chris Mitchell, 'Too Little Too Late: Can We Control Browser Fingerprinting?' (2020) 21(2) *Journal of Intellectual Capital* 165.

Second, browsers also have a strong motivation to compete with alternative platforms such as mobile browser applications. This results in considerable pressure to add new and powerful capabilities to the Web platform, to match those available elsewhere. Often, such new capabilities have a significant risk of fingerprinting. For example, it has been shown that the recently introduced Typed Array and High Resolution Time API features can be used to characterise system activity.[85] The information that this side channel attack exposes could aid in fingerprinting.

Third, in combination with other tracking mechanisms like IP addresses, even relatively simple forms of fingerprinting can effectively re-identify end users soon after they enter private browser sessions or they clear cookies. This effectively 'lowers the bar' so that sophisticated techniques are not required to meet the goals of tracking for Online Behavioural Advertising.

D *Regulation by law*

Legal regulation of fingerprinting has, to date, largely been confined to treating it as equivalent to cookies as a tracking mechanism.

1 *Europe*

While the GDPR is held to apply to the data collected through fingerprinting,[86] most European discussion of legal regulation of fingerprinting to date has occurred in the context of Article 5(3) of the ePrivacy directive and its explicit application to cookies,[87] which are motivated in terms of information stored on terminal equipment of users being 'part of the private sphere of the user requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms.'[88]

---

[85] Oren (n 45).

[86] See, eg, Irene Kamara and Eleni Kosta, 'Do Not Track Initiatives: Regaining the Lost User Control' (2016) 6(4) *International Data Privacy Law* 276.

[87] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* [2002] OJ L 201/37 [25], art 5(3) ('ePrivacy Directive').

[88] Ibid [24].

In 2014, the Article 29 Data Protection Working Party issued an opinion stating that 'Article 5(3) of the ePrivacy Directive is applicable to device fingerprinting.'[89] This requires treatment of fingerprint data in the same way that cookies are handled: namely, requiring consent and provision of 'clear and comprehensive information… about the purposes of processing.'[90] The stated purpose was to counter 'growing reports that third-parties are actively [fingerprinting] in an effort to avoid the consent requirement of Article 5(3).'[91]

The Working Party explicitly rejected arguments from the online advertising industry that fingerprints are not personal data, because considering them as such would be 'in contradiction to the purpose of processing for the delivery of personalised content and advertisements.'[92] However, they do allow for exemptions 'for the sole purpose of carrying out the transmission of a communication…' or when it is 'strictly necessary in order for the provider of [a] service explicitly requested by the subscriber or user…'[93] It goes on to explicitly allow fingerprinting for security enhancement without consent, invoking the latter exemption.[94]

The proposed ePrivacy Regulation incorporates this approach,[95] explicitly identifying audience measurement and fraud prevention as permissible without consent.[96] Notably, it also highlights the issue of consent overload, and mentions user-friendly and transparent controls to manage (or withdraw) consent as a potential solution — but only in a non-binding recital.[97]

---

[89] *Opinion 9/2014 on the Application of Directive 2002/58/EC to Device Fingerprinting* (Advisory Opinion) (Article 29 Data Protection Working Party, WP 224, 25 November 2014) 3 ('Device Fingerprinting Opinion').

[90] Ibid.

[91] Ibid 4.

[92] Ibid 7.

[93] Ibid.

[94] Ibid 10.

[95] Presidency, Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)'* (4 November 2020) 20 ('Proposed ePrivacy Regulation').

[96] Ibid art 8(1)(c)-(d).

[97] Ibid 20a.

Local privacy regulators in Europe are also examining fingerprinting; for example, the UK Information Commissioner's Office listed Web and cross device tracking as a priority area, explicitly mentioning fingerprinting,[98] and the Spanish data protection authority performed a survey on device fingerprinting in 2019.[99]

2 *United States*

In the United States, there has been considerably less legislative activity around fingerprinting. However, Solove and Hartzog argue that Federal Trade Commission privacy jurisprudence effectively forms a body of common law for the United States,[100] so I examine that.

The most relevant FTC actions were against firms who made statements about tracking that did not account for techniques other than cookies, under its power to enforce the prohibition against deceptive acts or practices affecting commerce.[101]

For example, the FTC's 2011 ScanScout complaint highlights the nature of Flash cookies as being 'not controlled through a computer's browser' so that 'if users changed their browsers' privacy settings to delete or block cookies, [they] were unaffected.'[102] Because ScanScout's privacy policy claimed that clearing cookies prevented tracking, the FTC brought an action for deceptive conduct against them.

Also relevant is the 2013 complaint against Aspen Way, where the FTC established that gathering consumers' personal information without notice is an unfair practice, in particular because the spyware that Aspen Way had installed on its client's computers could not be reasonably avoided.[103]

---

[98] Elizabeth Denham, 'Information Commissioner's Office — Technology Strategy 2018-2021' (Report, 2018) 9.

[99] Agencia Española de Protección de Datos , 'Survey on Device Fingerprinting' (Report, 2019) <https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital-EN.pdf>.

[100] Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (2014) 114(3) *Columbia Law Review* 583.

[101] Letter from James C Miller III to hon. John D. Dingell, 14 October 1983 <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

[102] Jon Leibowitz et al, *United Staes of America Federal Trade Commission and ScanScout* (Complaint, C-4344, 14 December 2011) <https://www.ftc.gov/sites/default/files/documents/cases/2011/12/111221scanscoutcmpt.pdf>.

[103] Edit Ramirez et al, *United States of America Federal Trade Commission and Aspen Way Enterprises* (Complaint, C-4392, 11 April 2013) <https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415aspenwaycmpt.pdf>.

Fingerprinting is likewise be difficult to avoid, and omission of notification would likely be judged a deceptive act; this may be one reason why modern privacy policies, like legislatures, have taken a technology neutral approach and used phrases like "cookies or similar technologies," thereby obtaining consent to fingerprint.

However, these complaints were not regarding fingerprinting specifically. That is not to say that the FTC is not aware of the technique; Bureau of Consumer Protection director Jessica Rich noted in a FTC workshop about cross-device tracking that 'there are no simple means for users to prevent [fingerprinting] – which, unfortunately, may be precisely why some companies have embraced this technology.'[104]

Due to the fragmented nature of privacy law in the United States, individual states might have additional protections. In California, the CCPA contains the concept of a 'probabilistic identifier' which would include fingerprinting, but does not distinguish their regulation from other forms of identification or tracking.[105]

The US response to fingerprinting therefore broadly mirrors Europe's, in that it is considered equivalent to cookies (albeit with much less legal constraint on both, except perhaps in California).

The FTC has shown some interest in assuring that users have effective control over tracking, with the staff report claiming the ill-fated Do Not Track mechanism would 'address concerns about existing choice mechanisms by "being more clear, easy-to-locate, and effective, and by conveying direct to websites the user's choice to opt out of tracking."'[106] To date, this has not eventuated.

VI Discussion

A *Fingerprints are not equivalent to cookies*

Because fingerprinting came to both the public's and regulators' attention after cookies became widely known as an online tracking mechanism, it is understandable that it has been most often framed in terms of cookies. However, this is a false equivalence, due to the stated differences in control and transparency.

---

[104] Jessica Rich, 'Beyond Cookies: Privacy lessons for Online Advertising (Speech, AdExchanger Industry Preview, 21 January 2015) 2 <https://www.ftc.gov/system/files/documents/public_statements/620061/150121beyondcookies.pdf>.

[105] *The California Consumer Privacy Act of 2018*, div 3 pt 4 Cal Civil Code § 1798.140.

[106] David Vladeck, Submission to Subcommittee on Commerce, Trade and Consumer Protection, United States House of Representatives, *Do Not Track* (2 December 2010) 16-17 <https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-do-not-track/101202donottrack.pdf>.

In past regulatory discussion, the privacy impact of cookies has sometimes been motivated by their storage of information on the user's computer without permission.[107] This concern is misled, even if it is a convenient fiction with which to regulate them: cookies are small, the total storage commitment for them is managed by the browser,[108] and that storage is cheap (to the point where no reasonable person would notice the space consumed by them on an even vaguely modern computer).[109]

Much more relevant is that a tracking mechanism which requires storing a value on the users' computer makes that mechanism potentially visible to and controllable by that user — embodying the very privacy-enhancing properties that fingerprinting lacks.

From the perspective of someone who wants to track online activity (for any of the purposes outlined), fingerprints thus have many advantages over cookies. They are much more difficult for the user to control, or even to know about. They are durable over significant spans of time, and they can adapt to changes in the capabilities of those that they wish to track.

That same lack of control and transparency dramatically increases the potential privacy impact of fingerprinting relative to cookies. When used for Online Behavioural Advertising, a tracking mechanism whose subjects cannot realistically control or even observe does not balance the privacy rights of individuals against the needs of advertisers and content producers; it is merely a means of avoiding architectural regulation, and perhaps a means of avoiding the attention of legal regulators as well.

Users' broad understanding of cookies as a tracking mechanism is not extended to fingerprinting, and even if there were, there is not a technical mechanism to opt out of fingerprinting globally; instead, users are required to discover the opt-out mechanism (usually embedded deeply in a privacy policy) and follow its directions on a site-by-site basis — often setting a cookie which might be cleared later. They then have to trust that the tracker will honour that commitment.

---

[107] See, eg, 'ePrivacy Directive' (n 87) [24]-[25].

[108] See, eg., 'Browser Storage Limits and Eviction Criteria', *MDN web docs* (Web Page) <https://developer.mozilla.org/en-US/docs/Web/API/IndexedDB_API/Browser_storage_limits_and_eviction_criteria>.

[109] See, eg, Tom Coughlin, 'Hard Disk Drive Quarterly Results and Projections', *Forbes* (online, 12 August 2020) item 7 <https://www.forbes.com/sites/tomcoughlin/2020/08/12/hard-disk-drive-quarterly-results-and-projections/>.

However, it is likely that many users will not understand these fine distinctions, and erroneously believe that clearing cookies, switching browsers, or using 'private mode' will protect them from tracking.

In other words, while the architectural regulation of cookies reinforces their legal regulation, the architectural regulation of fingerprinting is not as effective, and likely never will be. As such, legal regulation of cookies that treats fingerprinting as equivalent creates an incentive to use (and abuse) fingerprinting.

B *Fingerprints should be treated as sensitive information*

Intuitively, fingerprinting's lack of control and visibility has obvious parallels to sensitive data such as biometric data. Fingerprinting a browser or device is akin to taking a photograph of someone and then performing facial recognition, because obtaining consent for collection of the data relies on the collecting party's discretion, and because the data collected can be used to create a durable identifier that the person in question cannot easily change (in the case of fingerprinting, due to the economic cost and impracticality of replacing one's computer every time one opens a browser).

Because that identifier can be used to recognise that browser or device (and thus its user) anywhere on the Internet and can be appropriated to impersonate them, it intuitively follows that it is both powerful and sensitive.

However, it is unnecessary to rely on intuition alone to establish that fingerprints ought to be considered as sensitive data. Ohm shows that current legal regulations in various jurisdictions

> 'tend to focus on four factors in assessing whether a given piece of information seems sensitive: the possibility of harm; probability of harm; presence of a confidential relationship; and whether the risk reflects majoritarian concerns.'[110]

Browser and device fingerprinting can be argued to meet all four of Ohm's criteria. The first, third and fourth are common to all forms of online tracking. To wit,

(1) As discussed previously, all online tracking has a possibility of harm, because it can be used to build a profile of someone′s activity, including sensitive activities.

[110] Ohm (n 44) 1161.

(2) The nature of online activity is that it is bound to include data which has a duty of confidentiality attached; whether that be health data associated with one's browsing pattern. People now conduct much of their lives online, and as a result the nature of information is correspondingly personal and, at times, sensitive.

(4) Increasing public concern about online tracking has been documented widely,[111] and is reflected in a growing interest by regulators.

It is the second criteria where fingerprints are distinguished from other forms of online tracking. The lack of transparency and control incur a significant increase in the probability of harm. The relative ease of fingerprinting as well as the lack of accountability in its use means that unless regulated, many parties (including those performing Online Behavioural Advertising) have a strong incentive to use it in preference to cookies, where architectural regulation is more likely to mitigate these harms and help balance advertisers' interests against privacy rights.

C *Fingerprints require distinct legal regulation*

As discussed above, regulation of fingerprinting by norms and the market are not effective: architecture and law shoulder almost all of the burden.

However, architectural regulation of fingerprinting is limited; controls for cookies that are well understood (clearing cookies, tracking blockers, privacy mode) have no corresponding mechanism for fingerprinting. Anti-fingerprinting technologies have been shown to have modest effect, often being circumvented by newer techniques in what is described as a 'technological arms race'.[112] At an extreme, it implies that the only reliable way to change a browser or device fingerprint is to buy a new computer.

Furthermore, without legal regulation, browsers have strong incentives to take part in that war of attrition, likely interfering with the use of fingerprinting for fraud prevention, which is widely seen as legitimate. Although audience measurement and Web analytics are less clearly legitimate purposes, they would too be interfered with by architectural regulation, to the degree that it is possible.

---

[111] See, eg, Mary Madden and Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance* (Report, Pew Research Center, 20 May 2015) <https://pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

[112] See, eg, 'Device Fingerprinting and Targeted Marketing: The Next Digital Privacy Battleground?', *Hughes Hubbard & Reed* (Web Page) <https://www.hugheshubbard.com/news/device-fingerprinting-and-targeted-marketing-the-next-digital-privacy-battleground>.

It should also be noted that selective application of architectural regulation (e.g., on a site-by-site basis, as cookie blocking is often applied) would be problematic, because advertising networks could conceivably use fingerprinting for both fraud prevention and user tracking at the same time.[113]

In the current legal regulatory regimes of both Europe and the United States, fingerprinting is considered equivalent to cookies, despite having distinct qualities. Due to pressure from adjacent legal and architectural regulation of cookies and the comparatively attractive properties of fingerprinting, it is likely that use of fingerprinting will increase over time — resulting in a net loss of control over and visibility into online tracking. Users will have fewer architectural means of controlling tracking (as opposed to the pre-fingerprinting world of cookie-based tracking), less understanding of how tracking operates, and will be significantly more vulnerable to the effects of consent fatigue (because opting out of tracking would only be possible on a site-by-site basis).

Choice and control are held to be core principles within the framework of fundamental rights and freedoms, as applied to Web tracking.[114] This suggests that a legal response to fingerprinting that distinguishes it from cookies is necessary.

It is understandable that legal regulators might be reluctant to do so; 'technology-neutral' has been a watchword for some time in regulatory discussions. However, as Hildebrandt and Tielmans point out, '[i]f specific technologies interfere with the effectiveness of human rights, the legislator may have to address [those] technologies.'[115]

VII Potential legal responses

Legal regulation that treats fingerprinting as a distinct activity should ideally reset the balance between privacy rights and the interests of those performing online tracking to that intended by cookie-oriented legislation, while taking into account the imbalance in architectural regulation as explained above, as well as legitimate uses of fingerprinting. Below, I examine a few options for doing so.

---

[113] Brett Stone-Gross et al, 'Understanding Fraudulent Activities in Online Ad Exchanges' [2011] *Proceedings of the ACM SIGCOMM Internet Measurement Conference* 279.

[114] Working Paper on Web Tracking and Privacy: Respect for Context, Transparency and Control Remains Essential (Working Paper No 675.46.13, International Working Group on Data Protection in Telecommunications, 15-16 April 2013).

[115] Mireille Hildebrandt and Laura Tielemans, 'Data Protection by Design and Technology Neutral Law' (2013) 29(5) *Computer Law and Security Review* 509.

A *Banning fingerprinting*

An outright ban of fingerprinting would disallow its use for purposes that are widely seen as legitimate and necessary, such as fraud prevention. This approach can be discounted immediately.

B *Defining fingerprinting as sensitive data*

Formally classifying fingerprinting as sensitive data is an option that has the merit of aligning the intuitive nature of fingerprinting with its treatment by law.

In Europe, doing so would add the requirements of Article 9 of the GDPR over and above the lawful basis for processing personal data.[116] Under such a regime, use of fingerprinting for Online Behavioural Advertising could only take place if 'explicit consent' were obtained.

Although fingerprinting is already effectively required to be explicitly consented to by the ePrivacy directive, it is likely that a determination that fingerprints were sensitive would impose a requirement that online trackers 'clearly [inform users] about how and for what purpose [they] will use this data… [and] inform users in an exhaustive and clear way about the data that will [be collected] and the processing operations that will be carried out.'[117] It is arguable whether this is a higher bar than the 'specific information' standard currently set for obtaining consent related to cookies and related mechanisms.[118]

Use of fingerprinting for other purposes could be viewed as a legitimate interest on a case-by-case basis; for example, fraud prevention is already expressly allowed under the Article 29 Working Party Opinion on fingerprinting,[119] and it as well as audience measurement are allowed under the proposed ePrivacy regulation.[120]

---

[116] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, art 9.

[117] 'The Spanish DPA Fines Facebook for Violating Data Protection Regulations' (Web Page, 11 September 2017), *Agencia Española de Protección de Datos* <https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_09_11-iden-idphp.php>.

[118] 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (Working Document, Article 29 Working Party, 2 October 2013).

[119] 'Device Fingerprinting Opinion' (n 89) 10.

[120] 'Proposed ePrivacy Regulation' (n 95) 72.

In the United States, the FTC requires that 'where a company's business model is designed to target consumers based on sensitive data… [they] should see affirmative express consent before collecting the data from those consumers.'[121] This approach would continue to allow use of fingerprinting for purposes that were considered legitimate, while raising the visibility of its use for Online Behavioural Advertising by requiring such consent.

Classifying fingerprinting as sensitive data would therefore rely upon consent as the legal basis for Online Behavioural Advertising in both jurisdictions. However, based upon experience to date in Europe, it is not at all clear whether 'more consent' is an appropriate or effective way to balance privacy rights with advertiser interests. Even more tracking notices and consent dialogues is likely to result in additional consumer confusion, causing resignation in consumers — so-called consent fatigue.[122]

As a result, while classifying fingerprinting as sensitive data has some attractive aspects, it is likely not sufficient to balance privacy rights with advertiser interests.

C *Developing fingerprinting-specific legal regulation*

A refinement of considering fingerprinting as sensitive data would be to develop specific legal guidelines for its use, much like there are for biometric data in Europe[123] and some of the United States.[124]

Just as with biometric data, such guidance could define the purpose for which 'data are collected and processed, taking into account the risks for the protection of fundamental rights and freedoms of individuals.'[125]

Likewise, the issue of proportionality could be raised; it might be judged, for example, that fingerprinting is not essential for the purpose of Online Behavioural Advertising, therefore being inappropriate even with explicit consent, especially with less privacy-intrusive means available.

Controls could also be placed upon the retention and reuse of fingerprinting data, beyond those already required by applicable data protection legislation.

---

[121] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (Report, March 2012) 47.

[122] Bart W Schermer, Bart Custers and Simone van der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 16(2) *Ethics and Information Technology* 171.

[123] *Opinion 3/2012 on Developments in Biometric Technologies* (Advisory Opinion) (Article 29 Data Protection Working Party, WP 193, 27 April 2012) 3 ('Biometric Technology Opinion').

[124] See, eg, *Biometric Information Privacy Act*, 740 Ill Comp Stat § 14.

[125] 'Biometric Technology Opinion' (n 123) 7.

Arguments against regulation of data processing often take the position that doing so is paternalistic; that it undermines personal autonomy and hampers innovation.[126] While there is ongoing debate about the role of consent in data protection,[127] regulating the collection mechanism (in this case, fingerprinting) is distinct from processing, and should be examined based upon its own properties.

VIII Conclusion

Browser and device fingerprinting are techniques for online tracking, currently used for the purposes of fraud prevention, audience measurement, and Online Behavioural Advertising.

Current legal regulation of fingerprinting considers it to be equivalent to cookies, without considering its differences — namely, a comparative lack of control, transparency, and architectural regulation. Together, they argue for considering fingerprinting as a distinct privacy challenge, with the possibility of considering as sensitive personal data, and with a need for legal regulation to offset the deficit in effective architectural regulation.

Developing fingerprinting-specific legal regulation brings several challenges; it will very likely face the opposition of a well-resourced industry that has already learned how to engage with policy discussions from the history of cookies. However, it should be remembered that if fingerprinting becomes a widely used mechanism for Online Behavioural Advertising (and it already may have, thanks to the difficulties measuring it), maintaining the status quo will have the eventual effect of undermining any architectural regulation of cookies.

---

[126] Schermer, Custers and van der Hof (n 122) 179.

[127] See, eg, Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126(7) *Harvard Law Review* 1880.