MOW Data Governance and Accountability Positions

By James Rosewell

Overview

There are real consumer concerns related to privacy. Big Tech's proposals don't address them and primarily raise cost, stifle innovation, raise barriers to entry and shift the same business processing from servers onto consumers' local devices as part of their attempt to privatize the Open Web into yet another App Store. Big Tech knowing everything about everyone, with people having no choice, does not improve anyone's privacy.

1. Introduction

MOW was formed to ensure that the important discussions around improving privacy and competition result in policies that benefit society, rather than Big Tech. Big Tech's dominant narrative in mainstream media often states that privacy and competition are mutually exclusive.[1] In contrast, MOW believes that competition and data protection law can compliment one another in improving social welfare.[2]

---

[1] Apple, Complying with the Digital Markets Act (March 2024), stating that the DMA obligations have

> *"been made in the interest of promoting competition and consumer choice, but I believe it raises important privacy and security considerations…. While these changes bring new opportunities for competition, they will also inevitably create new and lucrative markets for malicious actors."*

https://developer.apple.com/security/complying-with-the-dma.pdf

CMA, Mobile Ecosystems Market Study Final Report (10 June 2022):

> *"Apple has argued that some of the suggested remedies might lead to privacy and/or security risks for users on its devices…. Where features are enabled in WebKit and used by Safari, but disabled for other browsers, this clearly does not support Apple's privacy and security arguments…."*

https://assets.publishing.service.gov.uk/media/63f61bc0d3bf7f62e8c34a02/Mobile_Ecosystems_Final_Report_amended_2.pdf

Kate O'Flaherty, Apple's New AI Security Move Explained, Forbes (24 June 2024):

> *"'We are concerned that the interoperability requirements of the DMA could force us to compromise the integrity of our products in ways that risk user privacy and data security,' Apple said."*

https://www.forbes.com/sites/kateoflahertyuk/2024/06/22/apples-new-ai-security-move-explained

[2] Wolfgang Kerber and Karsten Zolna, 'The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law, 54 European Journal of Law and Economics 217 (2022).

In contrast, MOW agrees with competition authorities that Apple[3] and Google[4] use false definitions of "privacy" to shield their anticompetitive conduct that does nothing to address people's true privacy concerns.

Improving digital privacy is laudable. MOW's mission is to ensure that as we address real privacy concerns, we retain an open, freely accessible decentralized internet, rather than one controlled and restricted by Big Tech. In short, regulators must prevent their attempts to privatize the web into yet another App Store.[5]

---

[3] CMA, Mobile Ecosystems Market Study Final Report (10 June 2022):

> *"We are concerned that Apple's current implementation of ATT is likely to result in harm to competition, make it harder for app developers to find customers and to monetise their apps, and ultimately harm consumers by increasing the prices or reducing the quality and variety of apps available to them….*
> *Apple justifies its restrictions on the grounds of user safety and privacy, as well as user expectations. However, we do not find these justifications compelling given that Apple allows other similar streaming services onto the App Store without these restrictions, and that cloud gaming services are present on the Google Play Store with no such concerns."*

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1138104/Mobile_Ecosystems_Final_Report_amended_2.pdf

United States v. Apple Inc., No. 2:24-cv-04055 (D.N.J. filed Mar. 21, 2024):

> *"Apple wraps itself in a cloak of privacy, security, and consumer preferences to justify its anticompetitive conduct. Indeed, it spends billions on marketing and branding to promote the self-serving premise that only Apple can safeguard consumers' privacy and security interests. Apple selectively compromises privacy and security interests when doing so is in Apple's own financial interest… In the end, Apple deploys privacy and security justifications as an elastic shield that can stretch or contract to serve Apple's financial and business interests…."*

https://www.justice.gov/opa/media/1344546/dl?inline

[4] CMA, Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals (11 February 2022):

> *"The announcements and actions prior to the issue of the [CMA's acceptance of Google's Commitments in the] June Notice showed (and created the expectation) that Google was determined to proceed with changes in the relevant areas, including by deprecating TPCs within two years of the announcements, in ways which advantage its own businesses and limit competition from its rivals….*
> *The CMA's preliminary view is that Google is likely to have been aware that these announcements, including the setting of a two-year deadline for deprecating TPCs, would adversely affect market participants and reduce competition. For example, studies cited by Google in the announcement of 22 August 2019 suggested that when advertising is made less relevant by removing TPCs, funding for publishers falls by 52% on average."*

https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf

[5] Recent disclosures of Google's internal documents reveal the goal of Privacy Sandbox was to "*successfully mimic a walled garden across the open web [so] we can protect our margins*." See United States v. Google. No. 1:21-cv-00392 (W.D. Tex. filed May 24, 2021).

https://www.texasattorneygeneral.gov/sites/default/files/global/images/TAC%20-%20Redacted%20Version%20(public).pdf

See also James David Campbell, Avi Goldfarb, Catherine E. Tucker, Privacy Regulation and Market Structure, Journal of Economic and Management Strategy (10 February 2015), finding that relying on consent for all data exchanges disproportionately impacts smaller organizations.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1729405

See also Anja Lambrecht, "E-Privacy provisions and venture capital investments in the EU (2017), finding uncertainty from vague privacy regulations increases costs, stifles innovation and reduces investment in data-driven businesses.

http://web.archive.org/web/20180601051456/https://www.ceps.eu/sites/default/files/Executive%20Summary%20-%20E-Privacy%20Provisions%20and%20Venture%20Capital%20Investments....pdf

and Jia, J., G. Z. Jin, and L. Wagman, The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment, Marketing Science 40(4) (1 March 2021), finding that over uncertainty from vague privacy regulation rules has negative effects on the financing of newer, data-related, and business-to-consumer European ventures, compared to their counterparts in the rest of the world.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912

The important protections of freedom of association, communication, and commerce are threatened by such dominant platforms who seek to become active gatekeepers, with immunity from their interference, their censorship and their broadcasting of misinformation, rather than their original role as facilitators among commercial actors in our digital economy.[6]

This article articulates MOW's privacy positions and proposes new remedies to address the varied privacy concerns people have.

2. MOW's Privacy Positions

2.1. Privacy is a human right where consumer expectations exist on a spectrum.

Big Tech's one-size-fits-all proposals do not adequately address different consumers' expectations and preferences.[7] While some people prefer more personalized experiences and seamless navigation across the open web and others prefer more disclosures and granular choices on the use of their Personal Data.[8] Although research consistently finds the vast

---

Garrett A. Johnson, Scott K. Shriver, and Samuel G. Goldberg, Privacy & market concentration: Intended & unintended consequences of the GDPR, Management Science, 69(10) (2023): 5695-5721, finding that larger firms that can more effectively gather consent have an advantage over smaller firms, such that Google and Facebook market shares increased post GDPR. https://ssrn.com/abstract=3477686

[6] The same principles the FCC aims to protect via its regulation of ISPs should be applied to the internet-access software required to connect to the internet (i.e. Operating Systems and browsers). Consumers would be harmed if Verizon blocked access to Apple Facetime, a competitor in telephony, or Comcast blocked access to Netflix, a competitor in connected television services. See FCC, Safeguarding and Securing the Open Internet (April 2024):

> "*[The FCC's new Order] This item would reestablish the Commission's authority to protect consumers and safeguard the fair and open Internet, which protects free expression, encourages competition and innovation, and is critical to public safety and national security…. [The Order would] Reinstate straightforward, clear rules that prohibit blocking, throttling, or engaging in paid or affiliated prioritization arrangements, and adopt certain enhancements to the transparency rule.*"

https://docs.fcc.gov/public/attachments/DOC-401676A1.pdf

Tarleton Gillespie, The Politics of "Platforms," New Media & Society, (December 2008). http://web.mit.edu/comm-forum/legacy/mit6/papers/Gillespie.pdf

In How Governments Shape Online Content Moderation (May 2024), Robert Gorwa provides useful insight into how platforms control communication among others for their own profit, rather than being neutral technology, when defining a "platform" as:

> "a *digitally enabled product that mediates relationships between two or more parties, usually featuring technical elements that allow third parties to build upon it or interact with it. This definition has three notable aspects: (1) it acknowledges technical features while noting that contemporary platforms are at their core* products *designed to generate profit for the companies that operate them; (2) it acknowledges that platforms are not simply neutral, and that 'a platform is a mediator rather than an intermediary'… and (3) it acknowledges that platforms are multi-sided markets that structure relationships between a number of different actors.*"

https://academic.oup.com/book/56385/chapter/448320701?login=false

[7] See differing expectations for different types of Personal Data in Eric Durnell, Karynna Okabe-Miyamoto, Ryan T. Howell & Martin Zizi, Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns with the Protection of Informational Privacy Scale (12 August 2020). https://doi.org/10.1080/10447318.2020.1794626

[8] CMA, Mobile Ecosystems Market Study final report, Appendix J (6 October 2022):

> "*Notably, Audiomack, a music streaming app, tested a variant of a pre-prompt screen which mentioned that users opting-in will allow the platform to remain free, resulting in a 64% opt-in rate.*"

https://assets.publishing.service.gov.uk/media/62a229c2d3bf7f036750b0d7/Appendix_J_-_Apple_s_and_Google_s_privacy_changes__eg_ATT__ITP_etc__-_FINAL_.pdf

See also IAB, The Free and Open Ad-Supported Internet: Consumers, Content, and Assessing the Data Value Exchange (29 January 2024): finding 69% of consumers prefer to provide Personal Data, rather than pay for access to media owners' content, while 91% would dislike paying for access to that content which is currently ad-funded.

majority of consumers prefer ad-funded access to digital content, there is an important minority for which the market should also offer options.[9]

Competition and the diversity of choice it supports must be available to meet diverse segments of society, which have different privacy preferences.

2.2. What does "privacy" mean?

Before discussing "privacy" further, we believe it is important to define what we are actually talking about. Everyone agrees that privacy is a multifaceted concept that is critical to a free and democratic society.[10] While privacy concepts apply to social interactions (e.g., communication), privileged relationships (e.g., doctor-patient, lawyer-client), physical locations (e.g., one's home), sensitive information (e.g., ethnic origin, religion, sexual orientation), and vulnerable classes of society (e.g., children), we should focus how we define online privacy regulations in relation to social expectations around the information flows that do and do not involve the above higher risk situations. In short, not all data poses substantive risk to individuals or society.

To advance discussions around true Personal Data protection, we should explore some of the confusions that frequently occur when discussing privacy concepts.

2.3. Privacy is not a property right

Discussions on improvements to the status quo should not be based on the "value" of privacy, as if it were someone's property. Regulators and researchers alike understand that data is not like property, as the use of data is non-rivalrous.[11] Moreover, basing privacy in property law

---

https://www.iab.com/news/consumer-privacy-research

[9] UK Ofcom, Adults' Media Use and Attitudes report (2022), finding 72% considered it an acceptable trade-off to share Personal Information when interacting with media owner properties, and only 21% of internet users were not happy for companies to collect and use their Personal Information, although even among this segment many were more willing to accept such data collection in exchange for ad-funded access to internet services.
https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes-2022/adults-media-use-and-attitudes-report-2022.pdf
See also survey distinguishing at least four segments related to what information is in question as to how many people would share their Personal Data with third parties to get a better deal online. https://www.telegraph.co.uk/business/2021/05/20/use-brexit-freedoms-kill-eus-cookie-popup-monster

[10] Danielle Keats Cintron, Daniel J. Solove, Privacy Harms, 102 Boston University Law Review 793, 818 (14 April 2022).
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222
See also Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vanderbilt Law Review 1609 (1999).
https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1988&context=vlr

[11] European Commission, Data Act: Commission proposes measures for a fair and innovative data economy, (23 February 2022):

> "*Data is a non-rival good, in the same way as streetlight or a scenic view: many people can access them at the same time, and they can be consumed over and over again without impacting their quality or running the risk that supply will be depleted.*"

https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113
See also ICO and CMA, Competition and data protection in digital markets: a joint statement between the CMA and the ICO (19 May 2021):

> "*data is non-rivalrous…. This means that data is not used up or deteriorated when it is copied. Once collected, sharing data does not decrease its value for the initial collector.*"

concepts, would tend to focus control over property on whomever invested more in enriching its value. Given online businesses invest far more than individuals to transform raw data into valuable assets, under a property-law basis of privacy protection their interests would more often than not outweigh those of individual's.[12]

Accordingly, we should look beyond the property-based notions inherent within the value or sale of data for true protections over individual privacy.

2.4. Privacy is distinguishable from security

Privacy is a related, but distinct concept from "security." Security prevents unauthorized access to and alienation from an asset. While data breaches may lead to privacy concerns, such violations result from lax security rather than internal data processing practices that may on their own give rise to reasonable concerns. Moreover, given human rights are inalienable, i.e. cannot be taken or given away, we should not seek to undermine them by confusing how to secure such rights against theft with their important protections under law.

Moreover, we should distinguish data handling practices (processing purposes) from organizations' security related to such data. "*The level of security should reflect the likelihood that the information could be used to cause harm and the severity of the likely harm*."[13] This context-specific analysis of risk should be proportional to organizations' obligations. When they collect sensitive and identity-linked Personal Information, greater obligations should be in place relative to non-sensitive and deidentified data.

2.5. Privacy is based in social norms of consumer expectations

Helen Nissenbaum provides a useful context-specific analysis of reasonable privacy expectations in relation to social norms that promote a society's values.[14] The UK Information

---

[12] Julie Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stanford Law Review 1373-1438 (2000).

> *"…I might "own" the data generated by my actions, and therefore the right to prohibit or condition its use by others. It is hard to see, though, how I would have the right to control what another gathers through his or her own diligence, even if what is gathered is information about me. If the criterion of ownership is effort, I will not always, or even most often, have the superior claim."*

https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?params=%2Fcontext%2Ffacpub%2Farticle%2F1819%2F&path_info=examined.pdf

[13] GDPR, Article 32, defines what degree of security is reasonable relative to:

> *"the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."*

Fred H. Cate, The Failure of Fair Information Practice Principles [from Chapter 13 of Consumer Protection in the Age of the Information Economy (2006).
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972

[14] Helen Nissenbaum, Privacy In Context: Technology, Policy, and the Integrity of Social Life (2010), holding that the "contextual integrity" of consumer expectations that derive from the "notion of appropriateness" in a given society's norms around interoperability of information flows and Personal Data handling:

> *"[A] right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information."*

Commissioner's Office (ICO) similar advocates a context-specific analysis in relation to the likelihood of risks to individuals' privacy.[15]

The goal of a data-driven society is to foster friction-free navigation and information flows, so long as the data in question does not pose a high likelihood of imminent substantive harm as perceived by a reasonable person.[16]

Given few adopt a Luddite perspective of returning to a pre-data-driven society,[17] we must look instead to how we properly address the needs of segments of society and varied desires among different audiences in relation to accessing online properties and the services they provide.

---

[15] ICO, Chapter 2: How do we ensure anonymization is effective? (October 2021):

> *"You should approach assessing identifiability risk by considering what is reasonably likely relative to the context…. You also need to frame this assessment in the context of the specific risks that different types of data release present…. Assessment of this risk is contextual."*

https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf

[16] See GDPR, Article 32 balance of interests relative to the ""the risk of varying likelihood and severity for the rights and freedoms of natural persons." See also Nicolas P. Terry, Struggling Paradigms In A Friction-Free World: Liability For Content In Post-Print Culture, Saint Louis University School of Law (2000).
https://scholarship.law.slu.edu/cgi/viewcontent.cgi?article=2156&context=lj
The long-standing legal "reasonable person" standard has frequently been used to balance respective interests in protecting speech rights (*see* Billy Raymond Counterman v. Colorado, 600 U.S. 66 (27 June 2023)). In short, negligence is the appropriate standard to apply to online data exchanges, which incorporates a constructive foresight of the likelihood of risk and severity of injury to a specific individual.

[17] The longstanding principle of data minimization rests on shaky ground, as when it is legal and reasonable to collect Personal Data limiting the collection would be unreasonable. If it is illegal and unreasonable to collect Personal Data, then reducing how much is collected does not address the true privacy concern. Even if we instead shift the analysis from collection to retention, this does not change the core analysis as to what is reasonable to continue to store for legally and reasonably collected Personal Data. Unlike many who believe data risk ripens with age, the risk is inherent in the original analysis of the likelihood and severity of harm such Personal Data poses to a specific individual. The duration of storage does not provide any insight into the security measures of an organization, nor does it alter whether the processing of Personal Data should reasonably occur. While most would agree that retaining sensitive information should have greater protections than non-sensitive Personal Data linked to a specific individual, few would argue that one's medical history should expire on a periodic basis.
See FTC Commissioner Rebecca Kelly Slaughter, Wait But Why? Rethinking Assumptions About Surveillance Advertising IAPP Privacy Security Risk Closing Keynote 2021 (22 October 2021):

> *"Understanding that the collection [of Personal Data] itself fuels the panoply of problems under the umbrella of "data abuses" helps point to a potentially more effective solution: bright-line purpose and use restrictions that minimize the data that can be collected and how it can be deployed. This data minimization approach would turn off the data pump and deprive the surveillance-economy engine the fuel it needs to run."*

MOW believes the appropriate analysis of risk rests in whether the Personal Data legally and reasonably collected serves a societal benefit that outweighs the rights of a specific individual. See GDPR, Recital 4.
See also Arushi Gupta, et al., The Privacy-Bias Tradeoff: Data Minimization and Racial Disparity Assessments in U.S. Government (FAccT '23 (June 12-15, 2023):

> "*Data minimization – the principle that entities should collect and retain only data minimally necessary to achieve their objectives – has meant that critical information needed to conduct fairness assessments is unavailable. We call this the emerging 'privacy-bias tradeoff.' As companies and regulators turn toward protecting individuals' information privacy via data minimization, we ask: How can we ensure that the lessons of algorithmic fairness are not ignored?*"

https://dl.acm.org/doi/pdf/10.1145/3593013.3594015
See also Omer Tene & Jules Polonetsky, Privacy in the Age of Big Data, 64 Standford Law Review 63 (February 2012):

> "*[A]n increasing focus on express consent and data minimization, with little appreciation for the value of uses for data, could jeopardize innovation and beneficial societal advances.*"

https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data

The UK ICO has provided additional guidance that the context-specific analysis of whether data is or is not Personal Data depends on the "in-whose-hands" test.[18] This guidance aligns to European rulings that reject the "ever possible" risk criterion of reidentification in evaluating whether information shared with a recipient that remains Personal Data in the hands of the sender, but anonymous in the hands of the recipient.[19]

Moreover, by focusing on likelihood and severity associated with the context of what data is processed we can better distinguish unintentional rule-breaking from intentional acts of harm.

2.6. Privacy is improved by competition, rather than in conflict with it

Both competition and data protection share a concern for social welfare and aim to ensure consumers benefit from the collection and use of data.[20] As discussed above, most consumers prefer access to free online services, rather than having to pay. However, the debate over privacy contains a false dichotomy that individuals must disclose their Personal Data to enjoy these free services.

- **Consent or pay**

Recent debates about "consent or pay" obscure two important points:

1) Some online *services* are necessary for modern life (e.g., search, communication, commerce),

---

[18] UK ICO, Chapter 2: How do we ensure anonymisation is effective?, (October 2021): 2-22:
"You also need to consider both the information itself as well as the environment in which it is processed. This will be impacted by the type of data release (to the public, to a defined group, etc) and the status of the information in the other party's hands…. This can sometimes be known as the 'whose hands?' question (ie what is the status of the information in the respective 'hands' of those who process it?)."
https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf

[19] European Court of Justice, CJEU - Case T-557/20, SRB v EDPS, ECLI:EU:T:2023:219 (General Court, 26 April 2023):
"The SRB submits that the data are rendered anonymous for a third party, even if the information allowing re-identification is not irrevocably eliminated and resides with the original processor, as long as the form in which the data are shared with that third party does not allow re-identification anymore or where re-identification is not reasonably likely.
The Court of Justice stated that that would not have been the case if the identification of the data subject had been prohibited by law or had been practically impossible on account of the fact that it would have required a disproportionate effort in terms of time, cost and man-power, so that the risk of identification would have appeared in reality to be insignificant (judgment of 19 October 2016, Breyer, C-582/14, EU:C:2016:779, paragraph 46).
Accordingly, it is apparent from the revised decision that the EDPS merely examined whether it was possible to re-identify the authors of the comments from the SRB's perspective and not from Deloitte's. Since the EDPS did not investigate whether Deloitte had legal means available to it which could in practice enable it to access the additional information necessary to re-identify the authors of the comments, the EDPS could not conclude that the information transmitted to Deloitte constituted information relating to an 'identifiable natural person' within the meaning of Article 3(1) of Regulation 2018/1725."
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62020TJ0557

[20] Case C-235/08 Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios ECR I-11125 (2006), finding that the benefit to society from improving the supply of credit history outweighed individual data protection rights associated with any sensitivity of data exchanges among businesses. However, MOW disagrees with the position that data protection regulations and competition ought to be analyzed independent of their impact on society.

2) Some online *content* should be controlled by media owners (e.g., video, audio, text), for which that owner controls monetization.

The platform services to find, navigate, access and interact with online content needs to be distinguished from property rights in the content itself. A social network may need to allow people to use platform services without monetizing their Personal Data.[21] However, such a platform should be able to condition access to commercial content on a purely ad-funded model.

To find a better balance in this ongoing debate, we ought to distinguish the *use* of the service (e.g., search or communication) from the *access* to media owners' commercial content. Freedom of speech should allow consumers to communicate with one another and with businesses, as well as enable businesses to restrict access to their commercial speech, so long as this does not illegally discriminate against protected classes of society. No one seriously argues that the New York Times must give its content away or that CNN must charge for access to their content. Each offers its own business model to attract visitors to their respective properties.

However, absent from the current debate is whether the data that fuels ad-funded access must always be linked to specific individuals or instead such interoperable data can serve this business-facing function in a deidentified state.

- **Interoperability vs Tracking**

Big Tech advances the position that there must be a negative impact to competition to "improve privacy." Importantly, they never address how they are improving true privacy issues, but instead attempt to redefine the term to mean "interference with technical interoperability". Their actual language defines "privacy threats" as all real-time cross-organizational exchanges of any data, which they pejoratively label "tracking" instead of the more accurate term "interoperability."[22] While Big Tech frequently refers to preventing "cross-context" data sharing, they fail to define what they mean by "context."[23]

---

[21] See Germany's Facebook/WhatsApp (Case No COMP/M.7217) Commission Decision 32014M7217 (3 October 2014), finding that Facebook abused its dominance in social networking by offering one-size-fits-all terms as a condition of using its core communication service for users, such that they could not provide meaningful consent regarding Facebook's combination of their Personal Data across all Facebook services and those of other business customers.

[22] CMA, Mobile Ecosystems Market Study Final Report (10 June 2022):

> "*[W]hile data protection law does not provide a legal definition of tracking, the CMA and ICO consider that Apple is conducting processing activities that can be characterised as tracking as described in the ICO Commissioner's Opinion on online advertising expectations.*"

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1138104/Mobile_Ecosystems_Final_Report_amended_2.pdf

[23] Apple states its Attribution solution "is intended to support privacy-preserving *measurement of clicks across websites or from apps to websites*. It is not intended to be used to track users, events, or devices *across those contexts*." (Wilander, 2021). How

Google's recent settlements with both Germany's Bundeskartellamt and 41 US State Attorneys General acknowledges that linking Personal Data across the contexts from all its consumer-facing services should not occur by default.[24] These same settlements allow Google to continue to use deidentified data that is not linked to the consumers' Google User Account (i.e. their authenticated identity). Apple too highlights the importance of using deidentified "random identifiers" not linked to Personal Data to support interoperability across its systems both in its public facing privacy policy and its submissions to competition regulators.[25]

Despite their own reliance on such deidentified data to support interoperability across their systems, Big Tech discriminates against rivals by imposing technical restrictions and policies that ignore this important distinction.[26] When setting up chokepoints on rivals' interoperability, Big Tech technically degrades the quality of service for rivals' information flows (e.g., slowing them down, interfering with the accuracy of information exchanged)[27] or blocks such communication

---

Apple suggests its linking of data "*across websites or from apps to websites*" without "track[ing]… events or devices" is left completely undefined.

[24] In Google's settlement with Germany's Bundeskartellamt (7 September 2023) reserved its rights to use deidentified data (i.e. that which is "*not combine[d with] Personal Data*"), especially for B2B purposes, without any change in user consent.

> "*A differentiation is made between users signed into a Google account and non-authenticated users…. here are Google services which can be used without signing in, but where no selection dialogues appear. In these cases users cannot choose between options concerning data processing before using the services.*"

https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2023/B7-70-21.pdf?__blob=publicationFile&v=3

In November 2022, Google relies on this same distinction in its settlement with 40 US State Attorneys General regarding its geolocation data collection, limiting obligations to Personal Data linked to a USER or their GOOGLE ACCOUNT, but excluding their device when not so linked. Google was also required to publish a disclosure:

> "*…including the fact that USERS cannot prevent the use of LOCATION INFORMATION in advertising by ADS PERSONALIZATION*."

https://www.attorneygeneral.gov/wp-content/uploads/2022/11/2022-11-14-PA-v.-Google-LLC-AVC-efile.pdf

Shortly afterwards, Google settled with the California State Attorney General under analogous terms. Google's My Ads Center currently states:

> "*Non-personalized ads on Google are shown to you according to factors like the time of day, device type, your current search or the website you're visiting, or your current location (based on your IP address or device permissions).*"

https://myadcenter.google.com/controls?hl=en

[25] Apple Privacy Policy (last accessed July 2024):

> "*Apple News delivers personalized content without knowing who you are. The content you read is associated with a random identifier, not your Apple ID…. When Apple does process or store data on our servers, it's associated with a random identifier — a long string of letters and numbers…. The content you read is associated with a random identifier, not your Apple ID.*"

https://www.apple.com/privacy

> "*If data is needed to make a service work, as far as possible Apple associates the collection with random identifiers and not the user's identity.*"

https://assets.publishing.service.gov.uk/media/62277271d3bf7f158779fe39/Apple_11.3.22.pdf

[26] The European WP29 identified Big Tech's self-serving exemption to blocking "third parties" but not their own third-party use in its deliberations that created GDPR. Working Party, 00909/10/EN, WP 171 (22 June 2010):

> "*[Blocking setting new cookies, but not reading existing third-party cookies] has as consequence that also cookies that have been set as first-party (when visiting the single website of, for example. a search engine or a social networking site) can still be read by that site when the user visits a site that has partnered with that first website.*"

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

[27] Compare Google's design of its User Agent Client Hints to the prior open standard of User Agent Strings that adds 100ms of additional latency for every first time visitor. Google, Privacy Sandbox Progress Report Prepared for the CMA (21 April 2023):

altogether by removing necessary local storage and client-server transmission functionality that their own business-facing solutions retain.[28]

When interfering with rivals' interoperability, Big Tech fails to distinguish when data is linked to specific individuals, making it by definition Personal Data, or when appropriate organizational measures are in place to safeguard these interoperable exchanges of information required for a decentralized ecosystem to flourish.

- **Big Tech's Self-preferencing exemptions**

Big Tech's proposed remedies to privacy concerns primarily aim to restrict others from access to raw data, offering to provide time-delayed, aggregated outputs often with fake data ("random noise") added for rivals' data-driven systems

Their public relations using their dominant positions to encode strategic definitions of privacy into information and market infrastructures.[29] Moreover, Big Tech's carefully crafted definitions of "privacy" exempt their own data collection and processing, under the "first party" exemption and "search" exemption.[30]

MOW agrees with competition regulators that Apple and Google frequently use false definitions of "privacy" to shield their anticompetitive conduct that does nothing to address people's true

---

"*We tested 60 sites (randomly selected) with an automation framework to load the sites hundreds of times. In aggregate, the rst page load across all sites appeared to incur an additional ~100ms in its FCP.*"
https://assets.publishing.service.gov.uk/media/644a36abc33b46000cf5e306/Google_s_Q1_2023_progress_report.pdf

[28] Compare Apple's SKAN attribution and Google's Attribution API that matches advertiser campaigns across the contexts of various app and website media owners' properties, while blocking access to storage of common match keys (e.g., cookie files or mobile advertising IDs).

[29] Michael Veale, Adtech's new clothes might redefine privacy more than they reform profiling, Netzpolitik (25 February 2022):
"*Apple and Google don't spare with privacy rhetoric around their initiatives, but conveniently these steps to reform adtech would install them as gatekeepers to insights about online users. The two companies would keep the data within browser and operating system infrastructure they entirely control.*"
http://web.archive.org/web/20220302054152/https://netzpolitik.org/2022/future-of-online-advertising-adtechs-new-clothes-might-redefine-privacy-more-than-they-reform-profiling-cookies-meta-mozilla-apple-google
See also Aaron Shapiro, Platform sabotage, Journal of Culterual Economy (23 February 2023):
"*The differential application of platform sabotage extends from these baseline conditions as a series of obstructive tactics designed to hinder rivals, manipulate consumers, befuddle regulators, and stratify the market for platform services.*"
https://www.researchgate.net/profile/Aaron-Shapiro/publication/368762412_Platform_sabotage/links/63fa79af0d98a97717b97d52/Platform-sabotage.pdf

[30] See also, Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt, Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels, FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency June 2022), p.508-520:
"*Apple itself engages in some forms of tracking and exempts invasive data practices like first-party tracking and credit scoring from its new tracking rules…. We find that Apple itself engages in some forms of tracking and exempts invasive data practices like first-party tracking and credit scoring from its new tracking rules…. Apple's Double Standards I: Making and Enforcing App Store Policies. Our analysis shows that Apple has a competitive advantage within the iOS ecosystem in various ways. First, it both makes the rules for the App Store and interprets them in practice. This is reflected in Apple's definition of tracking, which ostensibly exempts its own advertising technology.*"
https://arxiv.org/pdf/2204.03556

privacy concerns.[31] Apple's[32] and Google's[33] recent moves to further restrict rivals' advertising abilities removed obstacles for its own new advertising solutions to fill the void in solutions its conduct created.

Big Tech's technical interference with real-time, accurate interoperability aims to restrict rivals from offering improved solutions to consumers and to businesses.[34]

A reasonable balance of interests must apply to the collection and use of Personal Data. Data protection authorities understand that data protection is "not an absolute right."[35]

---

[31] United States v. Apple Inc., No. 2:24-cv-04055 (D.N.J. filed Mar. 21, 2024):

> *"Apple further locks-in the power of the iPhone by preventing the development of other disintermediating technologies that interoperate with the phone but reside off device.*
> *Ultimately, Apple chooses to make the iPhone private and secure when doing so benefits Apple; Apple chooses alternative courses when those courses help Apple protect its monopoly power."*

https://www.justice.gov/opa/media/1344546/dl?inline

[32] Hannah Murphy and Patrick McGee, Apple to boost ads business as iPhone changes hurt Facebook, Financial Times (21 April 2021):

> "*Apple will expand its advertising business, according to two people familiar with its plans, just as it brings in new privacy rules for iPhones that are likely to cripple the ads offered by its rivals, including Facebook…. If Apple cripples mobile advertising, then the App Store becomes the primary discovery point for apps again, and Apple decides how people use our iPhones, Apple decides which apps are the most popular.*"

https://www.ft.com/content/5527ddd1-77a8-4cd0-82fd-4568be5da80f

[33] See Google's proposals relying on

1) Differential Privacy (See Attribution Reporting, https://developer.chrome.com/docs/privacy-sandbox/attribution-reporting),
2) Multi-party computation (See SCAUP, https://github.com/google/ads-privacy/blob/master/proposals/scaup/mpc_servers.md) and
3) Encryption (See PAIR, https://blog.google/products/marketingplatform/360/engage-your-first-party-audience-in-display-video-360).

Each of these approaches limit access and aim to obfuscate specific events in the outputs other recipients receive, but offer no explanation as to why the dominant OS or browser ought to be trusted by either consumers or by businesses with the centralized collection of all input data necessary for downstream processing.

[34] CMA, Mobile Ecosystems Market Study Final Report ():

> *"A further barrier to competition is web compatibility…. The key barrier to competition in browser engines is Apple's requirement that other browsers on iOS use Apple's WebKit browser engine. In addition, web compatibility limits browser engine competition on Android (where Google allows browser engine choice). These barriers also constitute a barrier to competition in mobile browsers, as they limit the extent of differentiation between browsers (given the importance of browser engines to browser functionality)."*

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1138104/Mobile_Ecosystems_Final_Report_amended_2.pdf

[35] GDPR, Recital 4:

> "*The processing of personal data should be designed to serve mankind. 2The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*."

https://gdpr-info.eu/recitals/no-4

ICO and CMA, Competition and data protection in digital markets: a joint statement between the CMA and the ICO (19 May 2021).

> "It is important to note that data protection law recognises the function that personal data has for the economy and wider society, and as such the right to data protection is not absolute. The overall objective is to strike a balance. In an online setting, inventory is essentially empty space on a web page or mobile app, which can be filled with text (including links to other websites), images, and videos. between protecting these rights, ensuring processing is fair and lawful, individual rights are upheld, and organisations responsible for processing are accountable for the decisions they make and can demonstrate how they comply with the law."

2.7. MOW's proposed remedies to improve online privacy

All online harms are undesirable but remedies must be tailored to each harm, rather than impairing interoperability of data where the likelihood and severity of harm is outweighed by the societal benefits. Let's review three of the most common cited online harms related to navigating the open web and proposed tailored remedies to each.

- **Harm 1 – Illegal use of Sensitive Data**

Not all data is Sensitive Data. Whether data is sensitive or not depends on the likelihood and severity of risk to society from the use of such data. A challenge in today's networked economy is that the list of sensitive categories of information are not easily communicated with consumers or among businesses.

Remedy: The introduction of a standardized taxonomy of sensitive category information would enable enhanced disclosures and choices regarding their interactions with such content (e.g., expired security certificates).[36]

Given interoperable exchanges should rely on data rendered non-sensitive when possible, such labeling would help mitigate the risks to individuals by enabling pre-configured automation of such disclosures when interacting with content that involves such sensitive information.[37]

To avoid the risk of deplatforming or inadvertently unfunding digital properties that provide content, which may sometimes contain sensitive information, MOW proposes that transient processing of sensitive data to render it non-sensitive as an appropriate measure to mitigate risk to individuals. This aligns to recent US data protection regulations that rely on rendering data non-sensitive as an important mitigation measure.[38]

Of course, in cases where processing of Personal Data has a risk of causing a substantive life impact from the use of incorrect information, consumers should have greater control over such

---

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf

[36] See Google's automated warnings in an analogous context to properties that may cause consumers harm:
"*The site can misuse or abuse any information it receives, and could potentially attempt to install harmful software on your computer*."
https://support.google.com/chrome/answer/95617?+%22hl=%22+en+%28site%3Ayoutube.com%29#zippy=%2Cnot-secure-or-dangerous

[37] See Motion Picture Association's Film Ratings as an illustration of such a standardized taxonomy.
https://www.filmratings.com/Content/Downloads/rating_rules.pdf

[38] Federal Trade Commission, X-Mode Social, Inc.; Public Comment (18 January 2024), finding that rendering data deidentified or non-sensitive is an alternative to obtaining an individual's consent:
"*Respondents have the option to retain historic location data if it has obtained affirmative express consent or it ensures that the historic location data is deidentified or rendered non-sensitive.*"
https://www.federalregister.gov/documents/2024/01/18/2024-00928/x-mode-social-inc-public-comment

use and the right to request correction.[39] In summary, consumers have a right to access, request correction and deletion, and limit the uses of sensitive Personal Information.

- **Harm 2 – Unwanted Reidentification**

Not all data is Personal Data. Whether data is or is not "personal" depends on the "in-whose-hands" test, mentioned above.

Whether data is "deidentified" or Personal Data depends on whether the organization possessing the data has appropriate organizational measures to keep the data not linked to a specific individual's identity given its internal policies and public commitments to not reidentify, contractual prohibitions on recipients to not reidentify.[40]

As the European Court of Justice held in both Breyer (2016)[41] and SRB (2023), the appropriate risk analysis focus on the reasonable likelihood of whether the recipient of data has the legal means to reidentify a specific individual. In the 2023 Scania case (C-319/22), the Court of Justice of the European Union further clarified the appropriate analysis for determining whether an identifier constitutes Personal Data, specifically in relation to vehicle identification numbers (VINs). The court held that the VIN on its own is not Personal Data, even if it is Personal Data for those who have the reasonable means to link it to a specific individual.[42]

Remedy: All complex software systems require match keys (IDs) to operate. As described above, even Apple requires "random identifiers" to operate its businesses.

MOW agrees with Apple, but believes such identifiers should be visible, rotate periodically and be resettable by consumers upon a user-initiated action. Moreover, consumers should be able to navigate online content with a temporary match key assigned to their device (e.g., incognito

---

[39] See GDPR, Article 16 (right to recitifcation) as well as The Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.526. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/correction.pdf and Fair Credit Reporting Act (FCRA), 15 U.S. Code § 1681(i) - Procedure in case of disputed accuracy. https://uscode.house.gov/view.xhtml?req=granuleid:USC-1999-title15-section1681i&num=0&edition=1999

[40] California Consumer Privacy Act, 1798.140(m) "Deidentified" definition.

[41] Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779 (CJEU, 19 October 2016). The Breyer decision held that IP addresses do not on their own identify a specific individual directly. Instead, the ECJ ruled that an IP address only potentially can be used to reidentify an individual when the receiving organization has legal access to additional information to link the IP address to that individual's identity. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582

[42] European Court of Justice, CJEU - Case C-319/22, Gesamtverband Autoteile-Handel e.V. v Scania CV AB, ECLI:EU:C:2023:837 (CJEU, 9 November 2023)

> *"a datum such as the VIN – which is defined by Article 2(2) of Regulation No 19/2011 as an alphanumeric code assigned to the vehicle by its manufacturer in order to ensure that the vehicle is properly identified and which, as such, is not 'personal' – becomes personal as regards someone who reasonably has means enabling that datum to be associated with a specific person."*

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62022CJ0319

mode). This selection enables consumers to dissociate a specific session of activity from their default, temporary deidentified match key.

Scholars have long argued that pushing for individual control over all data processing is ineffective, given the practical inability for consumers to be meaningfully informed given the length and complexity of most disclosures,[43] as well as just plain annoying.[44]

Accordingly, interoperable exchanges of data should rely on deidentified match keys when possible. When interoperable exchanges of data depend on identity-linked match keys, consumers should have greater control.[45] By labeling when match keys and their storage is designated as Personal Data or Deidentified, we can mitigate risks to consumers without interfering with necessary business exchanges that do not involve Personal Data.

Google agrees with cookie labeling as an appropriate security measure (e.g., SAME-SITE), but applies the classification to the rejected notion of corporate ownership, rather than the risk of the data being collected and processed.

- **Harm 3 – Unwanted Personalization**

Not all people what personalized experiences. As described above, different segments of society have different preferences associated with their online experiences.

---

[43] Woodrow Hartzog, The Case Against Idealising Control, 4 European Data Protection Law Review 423 (2018):
"*The idealisation of control in modern data protection regimes . . . creates a pursuit that is actively harmful and adversarial to safe and sustainable data practices. It deludes us about the efficacy of rules and dooms future regulatory proposals to walk down the same, misguided path.*"
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299762
See also Julie E. Cohen, How (Not) to Write a Privacy Law, KNIGHT FIRST AMEND. INST. AT COLUM. UNIV. (Mar. 23, 2021):
"*Atomistic, post hoc assertions of individual control rights, however, cannot meaningfully discipline networked processes that operate at scale.*"
https://knightcolumbia.org/content/how-not-to-write-a-privacy-law
Ari Ezra Waldman, The New Privacy Law, 55 U.C. Davis Law Review Online 19, 38 (2021):
"*To the extent that second wave privacy laws offer individuals additional rights to access, correct, delete, and port information, they sit within a long tradition of privacy laws focused on atomistic personal autonomy and choice. Most scholars agree that this conception of privacy is outdated and incompatible with today's information ecosystem.*"
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3856598

[44] See UK Department for Science, Innovation and Technology Press Release (8 March 2023):
"*New data laws to cut down pointless paperwork for businesses and reduce annoying cookie pops-up are being introduced by the government today in Parliament.*"
https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr
Harry Yorke, Oliver Dowden: creating our own data laws is one of the biggest prizes of Brexit, The Telegraph (25 August 2021):
"*While cookies which pose a high risk to individuals' privacy will still require consent notices, the Culture Secretary says that many of them are "pointless" and should go.*"
https://www.telegraph.co.uk/politics/2021/08/25/oliver-dowden-creating-data-laws-one-biggest-prizes-brexit
Fred H. Cate, The Failure of Fair Information Practice Principles [from Chapter 13 of Consumer Protection in the Age of the Information Economy (2006): "*choice is often an annoyance or even a disservice to individuals*."
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972

[45] See US CAN-SPAM and Telemarketing Sales Rule.

Remedy: Consumers should be able to easily signal their preference regarding personalization to groups of recipients, without disclosing their identity, as to whether they want prior activity used to inform content matching.

> "*The ICO will present its vision for the future, where web browsers, software applications and device settings allow people to set lasting privacy preferences of their choosing, rather than having to do that through pop-ups every time they visit a website. This would ensure people's privacy preferences are respected and the use of personal data is minimised, while improving users' browsing experience and removing friction for businesses.*"[46]

This preference should be overridable on a context-specific basis (e.g., yes to Google Maps so I don't have to enter my home location, but no to Google Search as I don't want prior searches changing my future searches). Because consumers preferences may vary across groups, consumers should be able to override their preference signal on a group-specific or a business-specific basis.

- **Summary of proposed remedies**

The internet is governed by protocols that define how information is transmitted (e.g., TCP/IP), structured (e.g., DNS), rendered and interacted with (e.g., dynamic HTML).[47] The technical interoperability of these protocols enables automation and control across the decentralized system that comprises the open internet. What has been lacking to date is codifying additional metadata to help consumers understand when content is sensitive, when Personal Data is being collected, as well as the easy ability for users to signal their preferences concerning the personalization of their online experiences.

The pragmatic approach to mitigating risk is to enable users to set rules about their preferences, detect when sensitive content or data handling policies trigger those rules and take appropriate action (e.g., warnings that provide enhanced notice for visitors to consent or choose to navigate elsewhere).

3. Debunking Privacy Myths

3.1. Third Parties pose higher risk to individuals than First Parties

A common myth is that because consumers decide which consumer-facing properties to visit, but not the business-facing solution providers (aka "third parties") that support those

[46] UK Information Commissioner Elizabeth Denham (7 September 2021). http://web.archive.org/web/20210907001405/https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/09/ico-to-call-on-g7-countries-to-tackle-cookie-pop-ups-challenge

[47] Alexander R. Galloway, Protocol: How Control Exists after Decentralization, The MIT Press (2004). https://direct.mit.edu/books/book/2528/ProtocolHow-Control-Exists-after-Decentralization

properties, that the existence of such third parties creates a higher risk to individuals of privacy harms. Smaller organizations must by definition work with more solution providers to offer the same services and operate their businesses in competition with larger organizations.

However, consumers' privacy expectations do not fluctuate with the size of the organization with whom they interact. First parties pose identical harm to individuals from the abuse of Personal Data and hence both should be regulated equally. As the UK Information Commissioner's Office and CMA stated:

> *neither competition nor data protection regulation allows for a 'rule of thumb' approach, where intra-group transfers of personal data are permitted while extra-group transfers are not.*[48]

To exempt first parties from data protection regulations merely tips the scale in favor of vertical and horizontal mergers and acquisitions, without improving privacy for individuals.[49]

Remedy: Consumer default signals should not automatically exempt all First Parties, Search Engines or OS/browser manufacturers.

---

[48] ICO and CMA, Competition and data protection in digital markets: a joint statement between the CMA and the ICO (19 May 2021).
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf

[49] See ICO, Opinion on Data Protection and Privacy Expectations for Online Advertising Proposals (25 November 2021):

> "*As highlighted in the joint statement [with the CMA], a distinction is often drawn between the concepts of "first party" and "third party" when used both in web standards and industry definitions of data use. The Commissioner is aware of a view by market participants about how data protection law regards these concepts. For example, that first party has an inherently lower risk than third party. The Commissioner rejects this view….*
> *It is correct to note that the use of cookies and similar technologies presents lower privacy risks in some cases than in others. Some uses of first-party cookies may be regarded as carrying a lower privacy risk (eg the concept of "first party analytics"). However, this is not a general rule and does not necessarily apply to first-party cookies alone. The risks ultimately depend on the nature, scope context and purposes of the processing and how it is implemented…."*

https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf

See also ICO and CMA, Competition and data protection in digital markets: a joint statement between the CMA and the ICO (19 May 2021):

> "*76. A second area of potential tension arises where there is a risk of data protection law being interpreted by large integrated digital businesses in a way that leads to negative outcomes in respect of competition, e.g. by unduly favouring large, integrated platforms over smaller, non-integrated suppliers.*
> *77. For example, such risks could arise from an interpretation of data protection law in which transfers of personal data between different businesses owned by a single corporate entity – such as a large platform company – are in principle viewed as acceptable from a privacy perspective, while transfers of personal data between independently-owned businesses are not, even if these businesses are functionally equivalent to those of the platform and the data is processed on the same basis and according to the same standards.*
> *78. If implemented in practice, such an interpretation would clearly be problematic for competition, as it would provide strong incentives for companies to integrate horizontally and vertically in order to be able to process more personal data.*"

In contrast, MOW notes that the recent US federal privacy bill, American Privacy Rights Act of 2024, explicitly exempted consumer protections from both Search as well as "first-party advertising" in the definition from "Targeted Advertising."
https://www.commerce.senate.gov/services/files/E7D2864C-64C3-49D3-BC1E-6AB41DE863F5

High-quality, continuous, real-time interoperability, exchanging unaggregated data among businesses is necessary for competition within a data-driven economy.[50]

Per remedies above, such data is frequently not sensitive nor identity-linked. When it is, additional consumer controls should be available.

3.2. On-device processing gives consumers more control over data

On-device processing versus server-side processing can equally harm individuals. Consumers have no greater understanding or control over the inner workings of an operating system, browser or other vendors' software that operates on device (e.g., Microsoft Office on Windows) or in the cloud (e.g., Google Workspace on an Android-powered Chrome book).

- See by contrast, OS manufacturers' (e.g., Apple's and Google's) claims given such a distinction would give them greater control over ALL online data, regardless of risk.[51]
- The risk of data processing depends on the context of whether the data is sensitive and identity linked, or non-sensitive and appropriately safeguarded, rather than whether the software operates on a personal computer or on a server.
- Shifting business-processing costs onto consumers can drain their mobile batteries and is an unfair practice that should not happen by default.

3.3. Identity of people is distinguishable from random identifiers of objects

Some people confuse the random identifiers associated with objects as being indistinguishable from individuals' identity. Much of this confusion stems from Professor Latanya Sweeney, who tried to analyzed census records and concluded that only three common demographic data attributes were sufficient to make it possible to reidentify specific individuals across both datasets for 87% of the US population.[52]

However, such thinking conflates a few separate concepts. First, just as no addition of zeros can ever produce a non-zero number, no combination of non-identity linked information

---

[50] See Digital Markets Act, Article 6(10). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925

[51] Apple Response to the CMA's Mobile browsers and cloud gaming market investigation (23 February 2024):

> "*These updates [of Apple's processing consumer data]… include on-device machine learning to ensure user privacy, and expand on Apple's long-standing commitment to making products for everyone.*"

https://assets.publishing.service.gov.uk/media/6617ba00086b9d4398b95b0e/Apple_Non-confidential_Supplemental_Response_to_Issues_Statement_.pdf

[52] Sweeney L. k-anonymity: a model for protecting privacy. Int. J. Uncertainty Fuzziness and Knowledge-Based Systems (2002) 10: 557–570:

> "*Combinations of few characteristics often combine in populations to uniquely or nearly uniquely identify some individuals. For example, a finding in that study was that 87% (216 million of 248 million) of the population in the United States had reported characteristics that likely made them unique based only on {5-digit ZIP, gender, date of birth}.*"

could on its own reveal the identity of a specific individual. Any attacker must already possess the identity required to "reidentify" that individual.

Second, existence of unique patterns in a data set do not increase the likely risk of reidentification. Simply owning a car does not increase the likelihood that you will use it as a getaway vehicle to rob a bank. While it is technically possible to be so used, the likelihood you will plan a heist is not dependent on your ownership of a vehicle. To conflate the willful violation of the law (in this case robbery) with the possession of technology (e.g., a car) is to confuse the mere *possibility* with actual *probability*.

Finally, uniqueness alone in a dataset is not itself an issue. One should always assume any meaningful dataset will contain variance in the data. Thus, the potential risk depends only on whether the data being joined to the identity already in the bad actor's possession is innocuous or sensitive in nature.

Instead of focusing on whether data about objects are unique patterns, more pragmatic data protection instead focuses on what organizational measures are in place to mitigate risks to individuals.