The institutional framework required for the return to a genuinely Open Web

Introduction

Over 30 years, the web has transformed humanity's existence. The Movement for an Open Web (MOW) believes that this has been an overwhelming net positive for humanity. That is not to deny that there are grave & genuine harms that are perpetrated through the web today. We take these, and sovereign efforts to combat them, with the utmost seriousness. In this paper, we seek to present the argument that a return to a genuinely open web, not the network of walled gardens built by dominant platforms, can bring back its innovative spirit, can mitigate some of the personal, social and global harms we associate with the web, and will in any case make for easier regulation and enforcement. The paper proposes an institutional and regulatory framework centred around a separation of core browser functionality (e.g., navigation, content rendering) from the web application layer (e.g., authentication, fraud detection, content management, payment processing, etc.) by regulatory approval, active enforcement of pro-competitive measures to combat existing market power, and technocratic standard-setting for the web. The paper concludes with the argument that the openness of the web is a feature of the system as a whole, and needs, for its preservation, institutions charged with overall web architecture, and not competing institutions, each with responsibility for various aspects of regulation, like competition, privacy or content.

The Value of the Open Web

The Open Web (TOW) has been the defining innovation of the past 35 years and has brought benefits to humanity that are too rich & varied to enumerate or quantify fully. One study[1] that tries to track the size of the "Internet Economy" in the US has produced the following aggregate measures:

Table 6.2.1. National and Internet GDP

	2008	2012	2016	2020
Employment (millions)	3.05	5.1	10.38	17.65
National GDP ($ trillions)	$14.71	$16.20	$18.68	$21.18
Internet GDP ($ trillions)	$0.30	$0.53	$1.12	$2.45
Annual growth in national GDP		3%	2%	3%
Annual growth in internet GDP		16%	20%	22%
Internet GDP as percent of national GDP	2%	4%	6%	12%
Growth of internet GDP relative to national		5.3	8.3	6.7

[1] Deighton, J., & Kornfeld, L. (2021). *The Economic Impact of the Market-Making Internet: Advertising, Content, Commerce, and Innovation*. Published by the authors, October 2021.

Their definition of the “Internet Economy” may be expansive, and the US, as home of so many of the Web’s heavyweights, may have an even bigger internet sector than other countries, but 12% of GDP and growing at 22% is astounding. Moreover, the promises of natural language-based gen-AI, itself almost entirely dependent on content on TOW both for training and for useful tasks to perform, only adds to its value and significance.

Behind these dry numbers, we all of us know in each of our lives what is the centrality of TOW to wellbeing. Imagine the Covid19 epidemic without the web - lockdowns of the sort so many countries implemented are hardly imaginable without it. Remote work was possible for huge parts of the economy; the pivot to almost exclusively online socialising & entertainment made it bearable for many.

How this value derives from openness

MOW is a strong supporter of the benefits that TOW has brought, and believes that these have been due in very large part to the innovation that has been made possible by the fundamentally ***open*** architecture of the web.

Openness arose from the following combination of attributes:

- Policy requirements at the telecoms and networking level which led to the prevalence of largely un-metered access to bit flow, without regard to the content of the bits (e.g., net neutrality and fixed-fee pricing for internet data exchange between ISPs);
- A small number of light-weight technical standards to facilitate classes of applications above the networking layers (e.g., Simple Mail Transport Protocol for email, HTTP for web traffic, etc.);
- Permissionless innovation within classes of applications; for example, mail servers and clients can build on the standards and offer specific functionality; HTTP - a standard that has evolved over time - has accommodated all of the innovation on web services and web publishing that we have seen since 1990;
- Network effects, whereby the more standards were used, the more worthwhile it was for engineers and content creators to continue to use them because of tools, skills and a ready-pool of users and consumers.

These structural aspects of openness created the conditions for the dramatic fall in the variable costs of publishing and distribution; this in turn led to the proliferation of free-at-the-point-of-use content, much of it funded by data-driven advertising. “Data-driven advertising” refers to the standard collection and processing of event data to power business-facing solutions such as fraud detection, avoiding too many adverts for the same product or service (i.e. “frequency capping”), optimised content matching, and billing. There was extensive permissionless innovation with that content - perhaps most dramatically first in search, where Google’s PageRank algorithm was developed without the need for explicit cooperation from publishers, and then in social media, which innovated in ways for more people to share content easily and attractively.

The early web of permissionless innovation was uniquely meritocratic in the sense that content-creators and app-makers who developed products that satisfied end-user demands were able to thrive. In the web ecosystem before it was dominated by a small number of big platforms, openness was the engine of innovation. Interoperability within well-defined engineering standards led to cost minimisation, maximal re-use of effort (e.g., shared investment in common tools, like servers and browsers, linking and “mashups” for content-reuse, etc), and a huge amount of permissionless innovation. This openness was the result of a delicate balance between technical standards that have created and maintained interoperability, and, originally, a process of unfettered competition that allowed the best applications within each class to rise to the top.

How openness was eroded by platform dominance

Market power has been the fly in the ointment of the system of free innovation. The openness that arose in the 1990s and lasted for over a decade was the result of extraordinary historical circumstances and has turned out not to be resilient to market power. For example, as early as the first browser wars (1996-2002), Microsoft tried to apply the same tactics that had allowed it to dominate productivity software by reducing the interoperability of Internet Explorer while also exploiting its distributional advantage by bundling software into Windows. That threat to openness was parried at least in part thanks to the antitrust pressure on Microsoft in those years.

Google’s leverage of its search dominance into generalised dominance in advertising through the DoubleClick acquisition slowly built the next assault on openness. App and content makers, in order to succeed, no longer faced merely the sufficient condition that their product satisfied their users: it had to work for Google’s business model too. There were many aspects to this, from SEO-dominance of website design on TOW to Google taking a larger and larger share of content-providers’ display advertising revenues. Google’s assault on openness was copied and extended by Apple and to some extent Meta and Amazon.

A key factor of market dominance by on-line platforms is their huge economies of scale, scope and network externalities. They were formed by intervening in the underlying layers of the tech stack, in the wake of liberalisation of telecoms. The platforms’ ability to rely on *interconnection* between telecoms operators allowed them to build walled gardens of content that by-pass and directly mirror the reasons interconnection was mandated. Take messaging. Currently, features of Apple’s iMessage can only be seen by others with an iOS device: pushing families and groups of users to buy more of Apple’s devices. Interconnection between the underlying telecoms networks outlawed such discrimination in message functionality.

So, their scale and scope and network effects mean that many increases in efficiency allow them to pull further ahead of competitors. In a regulatory world that promotes efficiency almost as a goal in itself, they benefit from rules designed to promote efficient mergers and efficiency in supply and distribution; using increases in efficiency to justify their growth by acquisition and their efforts to vertically integrate entire supply chains. The huge downside that has not been seen by regulators is these vertical integrations deny rivals and markets vital data for innovation.

They were able to bend new laws to their will.[2] The GDPR has enabled them to accumulate huge footprints of usage and user's Personal Data. Google inferred from users' interactions with its products and responses to search queries the "quality" of web pages, and so improved its personal profiles for training its algorithms that are used for advertising.

Very early in its development of the search engine, Google understood that getting as close as possible to a complete view of who went where and when on the web was a key both to improved search and to domination in advertising.[3] The clickstream would help determine quality, and so allow Google to produce rankings that provided, for itself, the optimal balance of user-relevance and own-revenue maximisation.[4] Moreover, the same data combined with data from other sources such as user interactions with Google's products would help predict user behaviour, and in particular the probability of a consumer acting on an advertisement, this latter directly increasing Google's income.[5]

Acquiring clickstream data led Google to develop and acquire other products, including Google Analytics. It developed the Chrome browser and the Blink browser engine. Chrome allowed Google to set defaults for users such that, for the most part, direct data associated with a

---

[2] Apple's privacy lobbying has the most credibility, says campaign group, 9to5mac (6 June 2022): "Indeed, some US states are pushing forward bills that were largely written by lobbyists…. Those who seek to educate congressional offices on the bills say tech's fingerprints are clear through the talking points echoed by staff."
https://9to5mac.com/2022/06/06/apples-privacy-lobbying/
Note the Accountable Tech "campaign group", funded by Omidyar and anti-Twitter, has been criticized as receiving dark money from the Arabella Group's 4.7 billion-dollar influence fund.
https://www.influencewatch.org/for-profit/arabella-advisors .
See also Google sought fellow tech giants' help in stalling kids' privacy protections, states allege, Politico, (22 October 2021): "Google also bragged about "slowing down" new privacy rules in Europe that would apply to digital services like services such as WhatsApp, Facebook Messenger and Microsoft's Skype, according to internal documents quoted by the states…. We have been successful in slowing down and delaying the [ePrivacy Regulation] process and have been working behind the scenes hand in hand with the other companies," the complaint quoted Google executives as saying in a memo ahead of the meeting."
https://www.politico.com/news/2021/10/22/google-kids-privacy-protections-tech-giants-516834

[3] See information relating to the recent Google API documentation leak - https://sparktoro.com/blog/an-anonymous-source-shared-thousands-of-leaked-google-search-api-documents-with-me-everyone-in-seo-should-see-them/

[4] It is important to note that the two are not identical - for example, demoting the most relevant page for a search might induce the page owner to pay for placement in results, so increasing Google's own revenues while harming user experience. See Is Google Getting Worse? A Longitudinal Investigation of SEO Spam in Search Engines (2024).
https://downloads.webis.de/publications/papers/bevendorff_2024a.pdf?ref=404media.co and
7 Ways To Fix Organic Search Rankings Affected By Google's Latest Algorithm Updates (2021)
https://www.forbes.com/sites/forbesagencycouncil/2021/12/27/7-ways-to-fix-organic-search-rankings-affected-by-googles-latest-algorithm-updates

[5] Google uses Chrome browsing data to inform its Search ranking, which was a core motivation for building Chrome as an extension to its toolbar and NavBoost. See VP of Search, Pandu Nayak testimony of 6402-6473 @ https://thecapitolforum.com/wp-content/uploads/2023/10/101823-USA-v-Google-PM.pdf

specific browser could be collected.[6] Chrome's market dominance in browsers has given Google control of the most important method for consumers to navigate and interact with the open web. Chrome market power is leveraged in many ways - data collection is one since Google can know all of Chrome users' browser histories; the encouragement for users to use Chrome's wallet and its signed-in authentication mechanisms are others. Most recently, Google has tried to exercise its market power in advertising by restricting the amount of browser history and cookie data that rival B2B vendors can use through its so-called "Privacy Sandbox" modifications and a narrative that demonises B2B businesses.

Google's dominance has eroded the openness of the web by limiting the degree to which key pieces of user functionality are left to open, competitive processes. Because the browser is the main gateway to the open web, the absence of strong browser competition means that Google has a unique source of data about users' browsing histories. It can also bundle its Chrome core functionality with other Google products and exclude rivals without fear of being replaced. The bundled functionality attached to Chrome today includes discovery, navigation, communication, identity authentication, fraud detection, wallet-keeping, digital payments, and in-app web view.

Since all functionality embedded in the browser can replace or substitute for functionality that can exist at other locations in the web, if the browser does something even half well it will substitute for that taking place elsewhere. This is in part a consequence of browsers being the first step into a journey across the web, so a solution that takes less time and is presented with zero friction gains the identical market share as the browser itself regardless of the quality of the solution.

In each of the cases where functions are bundled in the browser, Browser dominance has allowed Google to strangle alternative providers.

- Discovery: it ought to be possible for users to have a rich configuration of search options through the browser, and yet defaults in Chrome all benefit Google search
- Navigation: it ought to be possible for users to access rival websites without increased latency (compared to interacting with Google's properties that bundle maps and navigation), yet AMP, Google's User Agent Client Hints, and other changes have slowed down rival publishers' user experience or increased the complexity associated with improving performance.
- Communication: it ought to be possible for smaller publishers to communicate in real-time across multiple business-facing partners to improve their business, yet Google interferes with their ability to store common interoperable data such as match keys and interferes with their ability to communicate in real-time, for example in its diverse assaults on header bidding.
- Account Identity & authentication: Chrome strongly encourages users to sign in to a Google account and link all devices for the same user to enjoy all the benefits of its disparate consumer-facing services - for example device synching - and that sign-in then becomes an easy default for sign-in on a great many non-google web properties. This

[6] For example, by default, Chrome will use typing in the address bar to suggest completions - thus typing and selected entries in the address bar could be recorded by Google.

ratchets Google's dominance further: independent properties adopt Google sign in because they know the majority of their users are on Google products … thus increasing the dominance. Google enjoys access to rich cross-site and cross-device information but restricts other publishers and marketers from using that same information

- Fraud Detection: Google operates ReCAPTCHA that detects fraud for other businesses, but restricts the same information from being accessed by rival fraud prevention solution providers.[7]
- Wallets and digital payments: payment details are by default stored in a Google wallet; this can be extended to preference its own digital payments and NFC-based payments on mobiles; these add to Google's proprietary data on individual shopping habits, strengthening its advertising market advantages.

Through browser dominance, Google is gradually building a "walled garden" of functionality where it sets the de facto rules for anyone wanting to offer services that depend on these building-blocks.

The W3C, the governing standards body for the web, defines the Browser as a "user agent" - software that retrieves, renders, and facilitates end-user interaction with web content. This is a foundational principle. The web's hypertext links allow websites to be found and the browser renders them visible to the user's computer. If a function comes ready-bundled into a browser, such as payments or password management or discovery, then there is less value or purpose in the user taking the step of searching or browsing the web; it has a ready-made response presented as part of the browser experience. Chrome's embedded features and dominant position has increasingly turned the browser into Google's agent. Its primary purpose has gone from helping users to helping Google. It now facilitates Google's profitable interaction with end-users, and not end-users' individual benefit-maximising interaction with a wider variety of the web content. The web has been centralised as a result.

Apple, of course, has done the same thing through its control of the entire hardware and software in its ecosystem. And Google and Apple together, through Android and iOS, have worked to more than replicate this level of control in mobile devices. Furthermore, Google's default search placement revenue share deal (of 36%) on Safari and iOS means that these two walled gardens are intricately inter-linked.[8] Under the deal, Google is the sole non-Apple recipient of clickstream data about Apple users' activity (with media owners' content).

---

[7] See https://www.termsfeed.com/blog/privacy-policy-recaptcha/ for an account of the data transfers to Google and the privacy terms covering that data.

[8] https://www.cnbc.com/2023/11/14/apple-gets-36percent-of-google-search-revenue-from-safari-alphabet-witness.html#:~:text=Google%20pays%20Apple%2036%25%20of,and%20the%20Department%20of%20Justice. See also: https://www.justice.gov/d9/2024-05/421631.pdf (slide 58) and https://thecapitolforum.com/wp-content/uploads/2023/11/U.S.A.-et-al-v.-Google-LLC-Nov-13-2023-Bench-Trial-Day-39-Morn-Sess-Transcript.pdf (page 111)

The open web, which thrived when anyone could innovate at any layer within given basic standards, has now largely disappeared because of the wall-building platforms.

How openness can be saved by active regulation and market design

The evolution of the open web shows that its original winning formula for openness is not resilient to being overturned by powerful market failures - notably due to network effects - that tend towards the emergence of walled gardens under laissez-faire policy. MOW believes that the open web is of greater social value than the walled garden web because it encourages innovation and competition, and is therefore more responsive to consumer and citizen desires in a way that walled gardens are not. Therefore, MOW believes that the original formula for openness - competition within settled technical standards, and level competition between standards until enough is understood to settle them - needs to be preserved and protected by regulation and careful market design.

Figure 1 below represents MOW's vision of how this can be done. MOW envisages:

- A set of competing core browser engines, all of them adhering strictly to narrow and settled technical standards for interoperability (narrower than current W3C scope), and strictly separated in ownership and incentive terms from other parts of the stack described below.
    - We envisage that these browser engines could be funded through Linux-foundation-style arrangements, with industry participants recognising the value as infrastructure of the browser engines and therefore providing the bulk of the funds, in much the same way that, for example, IBM, through its purchase and maintenance of RedHat, has funded important contributions to Linux development that has benefited all the distributions.[9]
    - Alternatively, if no one is willing to step up to the challenge of browser funding without a direct return, we can see that a functionally separate browser could be created and owned by the existing owners, who would continue to be responsible for capital expenditure (Google, Apple, Mozilla), with returns paid for through usage charges by other parts of the supply chain. To avoid the conflict of downstream users controlling the upstream supplier an "Openreach style" functional separation and non-discrimination set of obligations could be put in place.[10]
- The narrow browser engine technical specification would include APIs for building-block plugin services, provided by competing players, covering, for example:
    - discovery (search and advertising),
    - personal data permissions & control,
    - identity authentication and password management,
    - digital assistants (AI),

[9] See, for example, https://appdevelopermagazine.com/linux-in-the-enterprise-as-seen-from-ibm/

[10] The original proposal by BT Group plc (BT) in its competition law undertakings to Ofcom in 2005 was a functional/operational separation that unlike legal separation, does not involve asset divestiture, which was the basis for the formation of Openreach.

    - payments, etc.

  The intention would be that plugins would be provided in competitive markets, with antitrust authorities ensuring competition within each core area of functionality. For example, in search and advertising, the absence of a level playing field would be addressed by pro-competitive interventions in those domains. Extensions already exist on browsers, but by requiring the core browser to be limited in functionality, these marketplaces would develop their full potential. To remedy the issue of self-promotion and display in search pages, one option would be for Google to be required to provide access to its relevance engine on Fair, Reasonable and Non-Discriminatory (FRAND) terms so that alternative search engine result page (SERP) display businesses could be created. Current restrictions that prevent the combination of data feeds from multiple search engines would need to be prohibited; Content and applications would be built on top of this plug-in layer; application-builders could specify that specific plug-ins at the functional level were required to access their own functionality. For example, a publication might require a particular option to be configured into the browser for advertising and Personal Data-permissions, when access is conditioned upon authentication (e.g., New York Times). MOW advocates strict ownership separation between the app layer and the plugin layer.
- Specific legal and regulatory requirements for specific jurisdictions would be defined in terms of the functionality that was required, permitted or forbidden in the core browser engine, at the plugin layer, or in applications. For example, privacy regulation requiring an audit of Personal Data re-use could require certain features of all permitted “Personal Data permission” plug-ins, and could require all apps to employ those features within a given jurisdiction.
- Complexity for the end-user would be kept under control through the development of a market for “configurations” which would assemble modular blocks into fully-formed usable products. Under strict separation, all the layers would need to be assembled in order to create the equivalent of today’s browsing experience. A civil society group - like the Mozilla foundation - could offer its favoured “configuration” (and solicit funds to cover its costs). This configuration would be, behind the scenes, a script that collected and built a complete browsing package. A publisher might offer its own configuration, and indeed some of today’s platforms might offer configurations. However, MOW advocates for a strict ownership separation between configurations providers and app providers - platforms would have to choose their business layer.

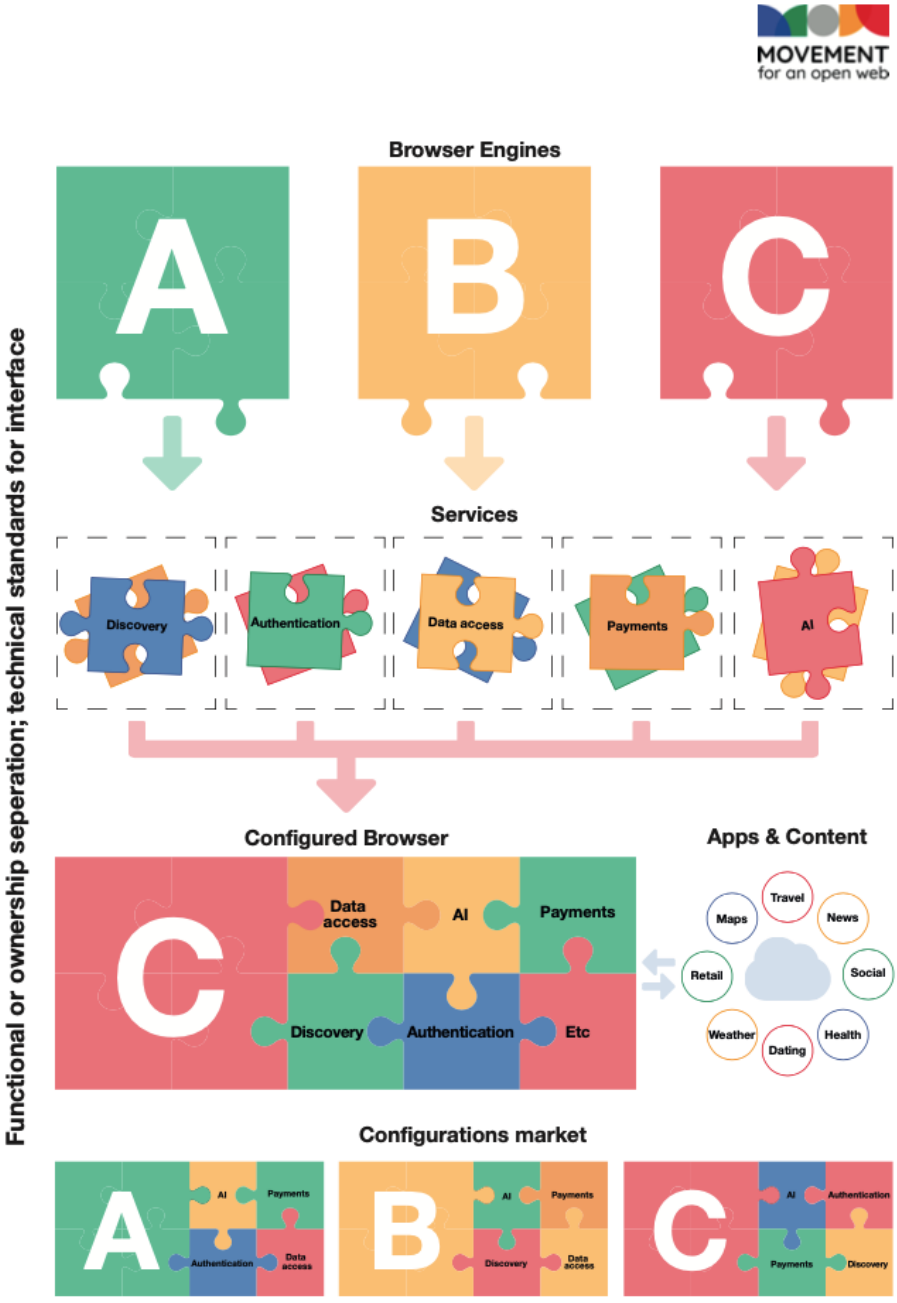

Figure 1. The top layer shows three competing Browser Engines. The next layer shows plug-in functions, like Search, Authentication, Personal Data Access Control. There are competing solutions and standards at this layer, although there is a common interface to the core browser engine - a call to a search function in the browser, for example, will have basic input/output standards defined. The two layers are characterised either by functional or full ownership separation. "Configurations" are bundles of options at the first two layers (and third, optionally), that create a working user experience. Apps and Content compete and are also characterised by functional or ownership separation.

This architecture would preserve the conditions of the open web - a level playing field for permissionless innovation within the context of narrow technical standards.

Such an architecture would itself require a governance structure that had the following features:

- A technical body - call it the “Web Browser Foundation” - to define core web-engine standards and browser functionality.
- Sovereign antitrust authorities across the OECD or the G7[11], building on current practice, could oversee the Web Browser Foundation to ensure that the functionality in the browser is quarantined and the browser operates as a tool for the user’s benefit, wherever the user is located worldwide.
- Browser unbundling would initially require browser and other functionality to be separated and policed across a non-discrimination boundary: the browser can be defined and policed and any technical upgrade to its function that is proposed by any market participant must be available, in source code, to all market participants. This avoids the problem of over-prescription of technical prohibitions in remedies, allows technology markets to develop and enables non-discrimination as a feature of forward-looking technology market developments. This remedies the problem of the current browser operating for the benefit of its owner and returns it to the purpose of the browser being the user’s agent. Sovereign authorities (democratic of otherwise) to define and enforce law and regulation over the plug-in and application layer within their own countries.
- MOW advocates for strict ownership separation between layers: the history of the destruction of the first Open Web shows that economies of scale, scope and network effects are powerful in cyberspace, and to enjoy their benefits without monopolisation, regulation needs to quarantine the browser and maintain the necessary non-discriminatory interoperability and openness.

Harms on the web today and how the proposed architecture for the open web mitigates them

The governance structure proposed above will ensure that web openness is maintained. However, the story of the web has not been one only of open innovation followed by market domination and the gradual erection of walled gardens. It has also been characterised by important harms to citizens, consumers and society never intended by the web pioneers or architects that go well beyond market harms. The existence of such harms are shared with any new technology. They do mean that there is a need for law and regulation to address them directly, and, crucially, a simultaneous need to maintain the overall coherence in the regulation of the open web.

[11] Other international bodies have been considered. A current concern with the development of telecommunication and internet standards is that non-democratic states should not be reinforced by remedies developed by democratic states. ITU standards were developed prior to the adoption of the UN and are now governed by UN agreement. Likewise the G7 could become the governing body for the Browser Foundation, an evolution of the current W3C.

Notable amongst these unintended consequences of the web have been the following:[12]

1. Public Safety
    a. Economic harm
        i. Misleading and deceptive practices or theft
        ii. Fraud, especially financial fraud targeting households, but also fraud targeting businesses and public institutions
        iii. Sale of illegal goods or services, especially medicine
        iv. Breaches of intellectual property rights
        v. Data and cyber security breaches or hacking for monetary gain
        vi. Illegal anticompetitive practices, such as data hoarding and restrictions by internet gatekeepers and strategic market status platforms, such that input data for data-driven solutions is under-used across competitive markets
    b. Information access harm
        i. Illegal restrictions on freedom of speech and expression
        ii. Censorship
        iii. Increased reach of misinformation, much of it malicious and orchestrated with elections, creating harms to democracy and social cohesion
2. Public Health
    a. Physical harm
        i. Publishing false or misleading medical information
        ii. Child abuse and Child Sexual Assault Material
        iii. Sexual exploitation
        iv. Slavery and human trafficking
        v. Encouraging self-harm
        vi. Encouraging harm of others and incitement of violence
3. Psychological harm
    a. Breaches of data protection or consumer protection laws
    b. Exposing age-inappropriate features, functions or content to minors
    c. Illegally discriminating against protected classes
    d. Hate crimes and the intentional infliction of emotional harm, including cyberbullying
    e. Consumer confidentiality and other privacy harms
        i. Identifier-focused harms, such as re-identification of deidentified information without appropriate notice and consent
        ii. Information-focused harms, such as unacceptable use of sensitive information without appropriate notice and consent
4. National Security
    a. Publishing illegal terrorist content or facilitating terrorist activity
    b. Communication and publication harms such as indecency, libel, etc

---

12 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

c. Increased ability to organise for intentional harm of society, especially terrorism & foreign enemy powers

MOW respects all sovereign efforts to appropriately mitigate these harms. Moreover, MOW believes that the technical and governance architecture proposed above for maintaining web openness will in itself mitigate some of these harms, and will in all cases make regulation more effective. Two examples are provided for illustration.

- Platforms, because they gather such a large share of the economic rents from advertising, have found it very profitable to create products that lead to greater time spent on-screen. Some of those products - especially the social networks - have been extremely susceptible to hostile-power information operations that can distort public elections. The open web that MOW advocates should reduce the information rents accruing to platforms, and therefore will both reduce the "exposure surfaces" that have been exploited in this way and increase the surface areas for disseminating good speech to counteract misinformation. This is an example of openness mitigating one of the harms of the current web.
- An Ofcom survey reveals that most consumers are not worried about sharing their purchasing and clicking data per se, but rather are concerned that any Personal Data that they do share is in safe hands.[13] In MOW's vision of the open web, a sovereign privacy regulator could respond to such public sentiment by requiring that the "Personal Data access control" plugin used in their jurisdiction should provide standard terms for Personal Data sharing and an audit functionality such that consumers (and enforcers) could determine automatically whether such information had been lawfully shared.[14] This would allow ready enforcement as well as increased transparency to consumers with the ability to automatically signal Personal Data sharing and personalization preferences (hence ending the cookie pop-up screen). In this example, the ability to mandate certain features for compliant plug-ins renders enforcement easier, and so one of the unintended privacy harms of the current web is mitigated.

How to maintain coherent regulation for openness when harms and externalities persist - the example of privacy regulation

Even if the open web architecture advocated by MOW does not entirely mitigate the harms that are done in cyberspace, a well-crafted architecture will help regulators with enforcement.

MOW believes that such regulation can be performed without compromising the basic architecture of openness. However, it is also possible to imagine mitigating policies that *would* compromise the openness we have described above. Openness is a valuable system-wide characteristic, and therefore needs to be defended by consideration of the entire web

[13] OFCOM 2022 Adults' Media Use and Attitudes survey. OFCOM has changed its survey question, and in its most recent survey, 71% of consumers are happy with status quo data sharing arrangements, against 9% unhappy. See https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-adults/adults-media-use-and-attitudes-2024-interactive-report/

[14] An example legal and technical implementation is provided by OPAL.

ecosystem, rather than any one aspect of it. There is therefore an important additional governance requirement in our proposed system: an institutional mechanism to ensure the right overall balance in the legal and regulatory tools deployed.

We will illustrate this with an examination of the case of privacy regulation. Privacy is a complex good and many of its dimensions are contested and valued differently in different cultures. Analytically, we can differentiate between four types of benefit that are sometimes collected under the "privacy" term:

1. The right to be left alone, undisturbed while in seclusion[15]
2. The ability to make decisions autonomously, for oneself, and not to be manipulated by misleading and deceptive practices.
3. The protection from harms to reputation that come from unauthorised disclosure of private, sensitive and confidential information
4. The ability to be treated anonymously, like everyone else, and not to be subject to illegal discrimination

International Treaty law as well as various domestic laws of different states protect aspects of all of these, and US law tends to place less emphasis on the second and the fourth.[16]

There are ways of promoting some of these aspects of privacy that would undermine the spirit of an open web. For example, a privacy regulator might consider that the most direct way to provide strong assurance against Personal Data sharing that might lead to reputational harms (conception 3 above) would be to impose onerous conduct and liability regulation such that only a few large platforms were able to participate in the advertising market. The regulator might develop policies that in effect banned the sharing of usage data for the purposes of the "search and advertise" plug-in, which would give a very strong advantage to large vertically integrated platforms with direct relationships with end-users. This might be an effective harm-mitigator from the narrow perspective of the needs of the privacy regulator, while also clearly undermining the level playing field of open standards that underpin the open web. From the perspective of an authority tasked specifically with addressing privacy harms, this might seem like a good regulatory solution. On the other hand, a competition-first approach that did not have

[15] As found in Article 8 UK Human Rights Act 1988 & Section 8 1948 European Convention on Human Rights.

[16] The United States Constitution does not contain any explicit right to privacy. However, The Bill of Rights expresses the concerns of James Madison along with other framers of the Constitution for protecting certain aspects of privacy. For example, the 1st amendment allows the privacy of beliefs, the third amendment protects the privacy of the home against any demands to be used to house soldiers, the fourth amendment protects the privacy of a person and possessions from unreasonable searches, and the 5th amendment gives the privacy of personal information through preventing self-incrimination. Furthermore, the 9th Amendment says that the enumeration of certain rights as found in the Bill of Rights cannot deny other rights of the people. While this is a vague statement, court precedent has said that the 9th amendment is a way to justify looking at the Bill of Rights as a way to protect the right to privacy in a specific way not given in the first 8 amendments. See also Article 8, European Convention on Human Rights regarding the right to respect one's private life . See case *Lloyd v Google* [2019], which follows successful settlements in *Vidal Hall & Ors v Google* [2015], regarding Google breaching its duties as a data controller and misused users' private information.

appropriate regard for the special status of privacy as a human right might be content to impose "light-touch" informational requirements on data-sharers - for example, requiring only terms and conditions to be published on what purposes were and were not being consented to.

The best solution in many jurisdictions and political cultures, however, is almost certainly not to have either a privacy-first approach or a competition-only approach, but rather to seek a coherent overall architecture. An example of this is the "trusted interoperability" solution proposed by the Open Preference Alliance project.[17] Under this proposal, a standard is developed which allows metadata to be attached to any data used on the web, with the metadata containing a link to the (standard, smart) contract under which it is shared, the type of data involved (perhaps with an indication to its degree of sensitivity). A privacy regulator could require that any Personal data exchanged on the web have this metadata attached to it,[18] and could even specify the range of acceptable contractual terms for sharing - including revocation rights, audit rights, etc to ensure that citizens were able to trace what Personal Data had been used by whom, and would have a simple way of revoking permissions.

Such a solution would not be chosen by a pure privacy regulator; and it would not be the choice of a pure laissez-faire, Chicago-style regulator confident in the actions of sovereign consumers. However, it is a solution that addresses a specific harm and preserves the architecture of TOW. Moreover, it would facilitate enforcement: anyone found using Personal Data without metadata at scale would be investigated and bad actors in the chain rapidly identified. Compliance against contractual terms could be monitored at large scale and automatically by the privacy regulator requiring specific audit routines and reports. The IAB's Transparency and Consent Framework provides many similar features.[19]

A more nuanced approach might also be possible. Regulation might come to recognise that not all data poses equal risks, and indeed some data might be Personal Data in the hands of one organisation or in one context, but not in another.[20] The OPAL approach might be the right solution for data that is not personal or sensitive - for example advertising tracking based on random identifiers. The privacy regulator might want to adopt a solution with even greater citizen control for Personal and Sensitive Data categories. One example for a standard with strong control mechanisms is Solid, the protocol devised by Sir Tim Berners Lee to allow personal access control for data where an individual or organisation truly wants granular control.[21] Regulation will need to consider speed, technical efficiency, business model requirements and

---

[17] See OPAL. See SWAN for details on the metadata format proposed. OPAL adds a standard contractual layer on top of these data and exchange standards.

[18] Instead, the regulator could treat with great suspicion any entity using data without the corresponding metadata, effectively ensuring similar outcomes.

[19] https://iabeurope.eu/transparency-consent-framework/

[20] ICO, Chapter 2: How do we ensure anonymization is effective? (October 2021) p. 11: *"the same information can be personal data to one organisation, but anonymous information in the hands of another organisation. Its status depends greatly on its circumstances, both from your perspective and in the context of its disclosure."*
https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf

[21] See https://www.w3.org/community/solid/

how much control is demanded by citizens for different categories of data in choosing a mandated data sharing architecture. Regulation might distinguish between sensitive categories of information deserving more robust safeguards and de-identification and less risky data that might require less robust - and less costly and restrictive - approaches. This suggests that the "Personal Data access control" plug-in could evolve into a regulated object that had more granular permissions than simply labelling data as personal or non-personal. It would maintain the ability for machine-to-machine assessment of Personal Data rights and responsibilities, and therefore continue to make audit and enforcement automated tasks.

This raises an important and more general institutional question: how are such overall coherent approaches to be ensured when each regulator is responsible for just one aspect of the entire system? The issue applies not only to privacy, but to all the unintended harms listed above and no doubt to others. When trying to combat election interference, should specialist regulators seek direct conduct regulation of platforms? Or should they instead require disclosure of information about the provenance of stories enabled through a "provenance" plug-in? Should "harmful but legal" content be limited through direct requirements on centralised platforms, or should mechanisms for greater parental control be required in the Personal Data access control layer? When many different agencies with different powers and responsibilities are all making decisions about the operation of the system, there is a clear danger that all of the decisions together will lead to incoherence and to poor choices when taken in the round.

MOW believes that it is always better to preserve the open architecture described and to regulate within the structure provided by it rather than to apply legislation and regulation that undermines that structure. However, in the UK, there is currently no body empowered to make the overall architectural choices for the open web as a whole, and no explicit criteria in policy for making these choices. The CMA is a specialist competition regulator that is allowed, in the context of a specific competition case to make decisions where, on a case-by-case basis, "benefits" to different public interests arise. So benefits to plurality of the media, security, diversity, or the environment may be considered in a suitable case under its DMCC powers.[22] MOW would welcome the CMA's DMU taking overall responsibility for web architecture and policy coherence in the UK, although we are concerned that the legislation only empowers the DMU with regards to the conduct of the large platforms. A proper regard to the systemic nature of regulatory choices needs to consider the behaviours of all actors within the system and all relevant public interests.

MOW believes that the UK - and other sovereigns - should explicitly designate a regulatory authority to have "architectural responsibility" for the web. They ought to make their regulatory

[22] The new Digital Markets, Competition and Consumers (DMCC) Act (2024) in the UK contains provisions that involves the CMA examining "benefits for consumers" when enforcing certain provisions under the Act (see ss. 19(10) and 29 regarding the imposition of conduct requirements and ss. 46 for pro-competition interventions). Lords Hansard and the CMA provided examples of benefits as "protecting user security or privacy, lower prices, higher quality goods or services, or greater innovation in relation to goods or services" (CMA (24 May 2024), Draft digital markets competition regime guidance, para 7.64)

decisions on the broadest possible public interest grounds. These architectural decisions should constrain the choices of individual domain regulators. In the UK, if the CMA takes on that role, then it should develop an architectural plan and guidelines for all regulators.