Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 84

Privacy and Security Implications of Regulation of Digital Services in the EU and in the US

Mikołaj Barczentewicz

2022

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Dr Mikołaj Barczentewicz is a Senior Lecturer (Associate Professor) in Public Law and Legal Theory at the University of Surrey School of Law, as well as the Research Director of the Surrey Law and Technology Hub. He is also a Research Associate at the University of Oxford, a Fellow of the Stanford Law School and University of Vienna Transatlantic Technology Law Forum, as well as a Senior Scholar at the International Center for Law & Economics.

General Note about the Content

Suggested Citation

This TTLF Working Paper should be cited as:
Mikołaj Barczentewicz, Privacy and Security Implications of Regulation of Digital Services in the EU and in the US, Stanford-Vienna TTLF Working Paper No. 84, http://ttlf.stanford.edu.

Copyright

Abstract

The goal of this project is to assess the data privacy and security implications of the 'new wave' of legislation on digital services—both in the US and in the EU. In the EU, the proposals for the Digital Services Act and the Digital Markets Act include provisions that have potentially significant security and privacy implications, like interoperability obligations for online platforms or provisions for data access for researchers. Similar provisions, e.g., on interoperability, are included in bills currently being considered by the US Congress (e.g., in Rep. David Cicilline's American Choice and Innovation Online Act and in Sen. Amy Klobuchar's American Innovation and Choice Online Act). Some stakeholders are advocating that the EU and US legislatures go even further than currently contemplated in a direction that could potentially have negative security and privacy consequences—especially on interoperability. I aim to assess whether the legislative proposals in their current form adequately addresses potential privacy and security risks, and what changes in the proposed legislation might help to alleviate the risks.

TABLE OF CONTENTS

1. Introduction

Increasing information privacy and security through the law is notoriously difficult even if that is the explicit goal of legislation. Thus, perhaps we should instead expect the law at least not to unintentionally *decrease* the level of privacy and security. Unfortunately, pursuing even seemingly unrelated policy aims through legislation may have that negative effect. In this paper, I analyse several legislative proposals from the EU and from the US belonging to the new 'techlash' wave. All those bills purport to improve the situation of consumers or competitiveness of digital markets. However, as I argue, they would all have negative and unaddressed consequences in terms of information privacy and security.

On the EU side, I consider the Digital Services Act ('DSA')[1] and the Digital Markets Act ('DMA')[2] proposals. The DSA and the DMA have been proceeding through the EU legislative process with unexpected speed and given what looks like significant political momentum, it is possible that they will become law. On the US side, I look at Rep. David Cicilline's American Choice and Innovation Online Act,[3] Rep. Mary Gay Scanlon's Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021,[4] Sen. Amy Klobuchar's American Innovation and Choice Online Act,[5] and Sen. Richard Blumenthal's 'Open App Markets Act'.[6]

I chose to focus on three regulatory solutions: (1) mandating interoperability, (2) mandating device neutrality (a possibility of sideloading applications), and (3) compulsory data access (by vetted researchers or by authorities). The first two models are shared by most of the discussed legislative proposals, other than the DSA. The last one is only included in the DSA.

[1] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/0361(COD)&l=en
[2] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act). https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/0374(COD)&l=en
[3] H.R. 3816, 117th Congress (2021-2022). https://www.congress.gov/bill/117th-congress/house-bill/3816
[4] H.R. 3849, 117th Congress (2021-2022). https://www.congress.gov/bill/117th-congress/house-bill/3849
[5] S. 2992, 117th Congress (2021-2022). https://www.congress.gov/bill/117th-congress/senate-bill/2992
[6] S. 2710, 117th Congress (2021-2022). https://www.congress.gov/bill/117th-congress/senate-bill/2710/

2. Risky regulatory solutions

2.1. Interoperability[7]

Interoperability of digital services is increasingly being presented as a potential solution to some of the problems associated with digital services and with large online platforms in particular.[8] For example, interoperability might allow third-party developers to offer different 'flavors' of social media news feeds, with varying approaches to content ranking and moderation. This way, it could matter less than it does now what content moderation decisions Facebook or other platforms make. Facebook users could choose alternative content moderators, delivering the kind of news feed that those users expect.[9]

The concept of interoperability is popular not only among thought leaders, but also among legislators. The EU Digital Markets Act, as well as the US bills by Rep. Scanlon, Rep. Cicilline, and Sen. Klobuchar, all include interoperability mandates.

---

[7] This section builds on my previous short text 'The Digital Markets Act Shouldn't Mandate Radical Interoperability' (Truth on the Market, 19 May 2021) https://truthonthemarket.com/2021/05/19/the-digital-markets-act-shouldnt-mandate-radical-interoperability/.

[8] Stephen Wolfram, 'Testifying at the Senate about A.I.-Selected Content on the Internet' (Stephen Wolfram's Writings, 25 June 2019) https://writings.stephenwolfram.com/2019/06/testifying-at-the-senate-about-a-i-selected-content-on-the-internet/; Mike Masnick, 'Protocols, Not Platforms: A Technological Approach to Free Speech' (Knight First Amendment Institute, 21 August 2019) https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech; Daphne Keller, 'If Lawmakers Don't Like Platforms' Speech Rules, Here's What They Can Do About It. Spoiler: The Options Aren't Great' (Techdirt, 9 September 2020) https://www.techdirt.com/articles/20200901/13524045226/if-lawmakers-dont-like-platforms-speech-rules-heres-what-they-can-do-about-it-spoiler-options-arent-great.shtml; Francis Fukuyama, 'Making the Internet Safe for Democracy' (2021) 32 Journal of Democracy 37 https://www.journalofdemocracy.org/articles/making-the-internet-safe-for-democracy/.

[9] Of course, this may have its own negative consequences in strengthening 'filter bubbles' and fuelling polarisation.

2.1.1. Privacy and security risks of interoperability

At the most basic level, interoperability means a capacity to exchange information between computer systems. Email is an example of an interoperable standard that most of us use today. It is telling that supporters of interoperability mandates use services like email as their model examples. Email (more precisely, the SMTP protocol) originally was designed in a notoriously insecure way.[10] It is a perfect example of the opposite of privacy by design.[11] A good analogy for the levels of privacy and security provided by email, as originally conceived, is that of a postcard message sent without an envelope that passes through many hands before reaching the addressee. Even today, email continues to be a source of security concerns due to its prioritization of interoperability.[12]

Using currently available technology to provide alternative interfaces or moderation services for social media platforms, third-party developers would have to be able to access much of a platform's content that is potentially available to a user. This would include not just content produced by users who explicitly agree to share their data with third parties, but also content—e.g., posts, comments, likes—created by others who may have strong objections to such sharing. It does not require much imagination to see how, without adequate safeguards, mandating this kind of information exchange would inevitably result in something akin to the 2018 Cambridge Analytica data scandal.[13]

---

[10] See e.g. Durumeric et al, 'Neither Snow Nor Rain Nor MITM… An Empirical Analysis of Email Delivery Security' (2015) *Proceedings of the 2015 Internet Measurement Conference*.
[11] See Article 25 of the Regulation (EU) 2016/679 (General Data Protection Regulation).
[12] See e.g. Sydney Li, 'A Technical Deep Dive into STARTTLS Everywhere' (Electronic Frontier Foundation, 25 June 2018) https://www.eff.org/deeplinks/2018/06/technical-deep-dive-starttls-everywhere.
[13] On the Cambridge Analytica scandal, see e.g. UK Information Commissioner, 'Investigation into data analytics for political purposes' https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

Imposing a legal duty on digital service providers to make their core services interoperable with any third party creates at least three categories of risks – as noted by Cory Doctorow and Benedict Cyphers:

1. Data sharing and mining via new APIs;
2. New opportunities for phishing and sock puppetry in a federated ecosystem; and
3. More friction for platforms trying to maintain a secure system.[14]

Friction in ensuring security

Beginning with the last point, a crude interoperability mandate could make it much more difficult for service providers to keep up with the fast-evolving threat landscape. For example, it may seem a good idea to require service providers to submit all changes to their interoperability standards (interfaces) for external review, possibly by a public authority.[15] This could potentially help to ensure that service providers do not 'break' interoperability or discriminate against some third-party services that would want to benefit from it. However, imposing such a requirement would introduce delay in responding to new threats, potentially putting user data at risk. When it may take seconds to exfiltrate millions of user profiles, delaying security patches by weeks or even days through regulation is unacceptable.

'Phishing and sock puppetry'

True interoperability of digital services would mean a two-way exchange of information. For online platforms like social networks this would mean that e.g. a Facebook user could

[14] Cory Doctorow and Benedict Cyphers, 'Privacy Without Monopoly: Data Protection and Interoperability' (Electronic Frontier Foundation, 12 February 2021) https://www.eff.org/wp/interoperability-and-privacy.
[15] An example of such a rule can be found in Rep. Scanlon's bill and I discuss it below.

interact with users of other interoperable platforms as if they were Facebook users today (exchange direct messages, see their posts, add comments and so on). Doctorow and Cyphers recognized that this would mean that any identity controls (e.g. Facebook's requirement to use real names) could easily be undermined if criminals or state actors run or control their own interoperable platforms. Those in control of such a platform could appear to users of other platforms as their friends in an attempt to hack them (e.g. phishing through direct messages). Such deception happens already on major online platforms, but those platforms are legally free to adopt measures to counteract it. A broad interoperability mandate would disallow service providers from vetting other providers and from imposing own identity requirements (e.g. requirement of using real names).

General data sharing risks

Data sharing risks stem from the fact that effective interoperability requires sharing of sensitive data between different service providers through new two-way real-time interfaces (application programming interfaces – APIs). Cory Doctorow and Benedict Cyphers, in a paper for the EFF, put forth a plan endorsing broad interoperability mandates.[16] But, admirably, they acknowledge the important security and privacy tradeoffs such a mandate would impose. Promoters of the bills analyzed herein frequently do not account for these costs, thus, it is worth analyzing these harms from the perspective of proponents of interoperability mandates. Doctorow and Cyphers are open about the scale of the risk: '[w]ithout new legal safeguards to protect the privacy of user data, this kind of interoperable ecosystem could make Cambridge Analytica-style attacks more common.'[17]

[16] Doctorow and Cyphers, 'Privacy Without Monopoly'.
[17] Doctorow and Cyphers, 'Privacy Without Monopoly' 28.

The Cambridge Analytica analogy illustrates the risks well. The personal data that Cambridge Analytica eventually used was collected through a Facebook app created by an academic researcher.[18] 270,000 people used this app and expressly gave the app permission to access their account information, including information about their Facebook contacts. This is how the app's author collected data on over 50 million Facebook users.

A potential future Cambridge Analytica could benefit from a poorly drafted interoperability mandate. Today, Facebook can and does stop third-party developers who try to exfiltrate data from the platform in violation of Facebook's terms. Some even believe that Facebook does so too vigorously.[19] But under an interoperability mandate, Facebook may be prevented from vetting and denying access to third parties as long as a user clicks 'yes' in a consent popup. And users may habitually click 'yes' in consent popups irrespective of any 'dark patterns' that would nudge users to authorise the desired action ('popup fatigue').[20] This is understandable: users may simply want to access the desired functionality (e.g. play a game) and may not be willing to invest enough time and effort to discover the consequences of what exactly they are authorising.

Thus, one risk is that users will authorise interoperability to the extent that may later surprise them, even if the third-party service providers provide all necessary information in an accessible and intelligible form. It may just be that users will only start caring about the consequences of their choices once they materialise, but not before making the choice.

---

[18] See also Kurt Wagner, 'Here's how Facebook allowed Cambridge Analytica to get data for 50 million users' (Vox, 17 May 2018) https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data.

[19] Mitch Stolz and Andrew Crocker, 'Once Again, Facebook Is Using Privacy As A Sword To Kill Independent Innovation' (Electronic Frontier Foundation, 20 November 2020) https://www.eff.org/deeplinks/2020/11/once-again-facebook-using-privacy-sword-kill-independent-innovation.

[20] See e.g. Cristian Bravo-Lillo et al., 'Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It' (2014) *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS)*; Anthony Vance et al., 'Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments' (2018) 42 *Management Information Systems Quarterly (MISQ)* 355.

However, it is unrealistic to expect all third-party service providers to obey the rules, including rules on acting in accordance with unstated user expectations. Some third-party providers may simply want to push the boundaries of what is allowed in good faith, due to (potentially erroneous) belief that the users will be better served this way. But some will intentionally engage in illegal, even criminal, activity.[21] Such actors may come from foreign jurisdictions (outside of the EU and the US), which could render ex post enforcement of legal rules against them particularly difficult.

2.1.2. How can the risks be addressed?

What could be done to make interoperability reasonably safe? There are several constraints that an acceptable solution should address.

Constraints

First, solutions should be targeted at real users of digital services, without assuming away some common but inconvenient characteristics. In particular, solutions should not assume unrealistic levels of user interest and technical acumen. As discussed above, users may not care enough about privacy and security settings when authorising interoperability *until* some negative consequences materializes. It is telling that supporters of interoperability mandates like to present as models services used by exceptionally motivated and informed

[21] As the OECD noted: 'Even where individuals and organisations agree on and consent to specific terms for data sharing and data re-use, including the purposes for which the data should be re-used, there remains a significant level of risk that a third party may intentionally or unintentionally use the data differently.' OECD, 'Enhancing Access to and Sharing of Data. Reconciling Risks and Benefits for Data Re-use across Societies' (2019) ch 4 'Risks and challenges of data access and sharing' https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en.

users, which are also small-scale (e.g., Mastodon) or have unacceptably poor usability for most of today's Internet users (e.g., Usenet).[22]

Second, solutions must address the issue of effective enforcement. Doctorow and Cyphers argued that there is a 'need for better privacy law' to make interoperability safe.[23] However, somewhat surprisingly Doctorow wrote soon after that 'the existence of the GDPR *solves* the thorniest problem involved in interop and privacy'.[24] Mere existence of any laws does not solve any problems. Problems can be solved if such legal rules are followed, and this requires addressing the problem of procedures and enforcement.

In the EU, the current framework and practice of privacy law enforcement offers little confidence that misuses of broadly-construed interoperability would be detected and prosecuted, much less that they would be prevented.[25] This is especially true for smaller and 'judgment-proof' rule-breakers, including those from outside the European Union. In the US, no such privacy framework exists on the federal level and the state laws like California Consumer Privacy Act face similar enforcement problems like the EU GDPR.

If the service providers are placed under a broad interoperability mandate with non-discrimination provisions (preventing effective vetting of third parties, unilateral denials of access and so on), then the burden placed on law enforcement will be mammoth. It could take just one bad actor, perhaps working from Russia or North Korea, taking advantage of

[22] 'mastodon' https://github.com/mastodon/mastodon; https://en.wikipedia.org/wiki/Usenet.
[23] Doctorow and Cyphers, 'Privacy Without Monopoly' 33.
[24] Cory Doctorow, 'The GDPR, Privacy and Monopoly' (Electronic Frontier Foundation, 11 June 2021) https://www.eff.org/deeplinks/2021/06/gdpr-privacy-and-monopoly.
[25] See e.g. Communication from the Commission to the European Parliament and the Council, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation' COM(2020) 264, 24 June 2020 https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf; Bureau Européen des Unions de Consommateurs, 'The long and winding road: Two years of the GDPR: A cross-border data protection enforcement case from a consumer perspective' (5 August 2020) https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf.

interoperability mandates to exfiltrate user data or to execute a hacking (e.g. phishing) campaign, to cause immense damage. Of course, such foreign bad actors would be in violation of the EU GDPR, but that is unlikely to have any practical significance.

It would not be sufficient to allow (or require) service providers to enforce merely technical filters like a requirement to check whether the interoperating third parties' IP address comes from a jurisdiction with sufficient privacy protections. Working around such technical limitations does not pose a significant difficulty to motivated bad actors.

The Open Banking solution

Probably the only solution that could potentially address the information privacy and security concerns in interoperability of digital services, without significant technological changes, would be to follow the example of the UK Open Banking regime.[26] As described by the UK's Competition and Markets Authority:

> Open Banking enables consumers and small and medium-sized enterprises (SMEs) to share their bank and credit card transaction data securely with trusted third parties who are then able to provide them with applications and services which save time and money.[27]

[26] On Open Banking, see e.g. Open Banking Implementation Entity, 'Open Banking' https://www.openbanking.org.uk/; Sam Bowman, 'Why Data Interoperability is Harder Than It Looks: the Open Banking Experience' (CPI Antitrust Chronicle, April 2021) https://laweconcenter.org/wp-content/uploads/2021/06/CPI-Bowman.pdf; Geoffrey A. Manne and Sam Bowman, 'Issue Brief: Data Portability and Interoperability: The promise and perils of data portability mandates as a competition tool' (International Center for Law & Economics, 10 September 2020) https://laweconcenter.org/resource/issue-brief-data-portability-and-interoperability-the-promise-and-perils-of-data-portability-mandates-as-a-competition-tool/.

[27] Competition and Markets Authority, 'Update on Open Banking' (5 November 2021) https://www.gov.uk/government/publications/update-governance-of-open-banking/update-on-open-banking.

Open Banking was introduced in 2017 and is a heavily regulated interoperability scheme, which its own special oversight body — the Open Banking Implementation Entity (OBIE). One of the key lessons from Open Banking according to Manne and Bowman is that

> Open Banking has been costly and time-consuming to implement. This is despite the fact that the data involved—chiefly transaction history and account balance data—is relatively simple and does not differ between different banks. The main difficulties have been around security, user authentication, and the authorization of new third-party services, and it has taken ongoing monitoring by a new agency set up by the CMA and several re-iterations to get these right, and may require more in the future. For services where the data is more sophisticated and unique to each service, the cost of implementing data portability and/or interoperability may be commensurately higher.[28]

Applying the Open Banking analogy to digital services in general could mean that:

1. There would likely be a need for a regulator to set the technical standards, to oversee the scheme, and possibly to enforce the rules in case of violations.
2. To be able to participate, any potential interoperating party would have to undergo expensive and thorough regulatory vetting (of the kind that financial institutions need to be allowed to operate).

Among the main problems in applying the Open Banking analogy to digital services in general is that Open Banking applies to relatively simple and homogenous data (e.g. bank transactions). Whereas, even the services offered by the largest providers are much more varied and continuously evolve. Imposing detailed technical data standards, like in Open Banking, would stifle innovation. Given that some standardisation of data formats is likely

[28] Manne and Bowman, 'Issue Brief: Data Portability and Interoperability' 23.

to be a feature of any interoperability mandate, this may be a sufficient reason not to adopt an interoperability mandate, but this issue is beyond the scope of this paper.

The second feature of requiring all participating parties to undergo regulatory approval modelled on financial institutions could contribute significantly to addressing the problem of bad actors or of insufficient motivation to follow privacy and security rules. However, some proponents of broad interoperability may object that this could partially defeat the purpose of interoperability mandates, because few 'two guys in a basement' start-up teams could benefit from it. It could be said in response that perhaps the risks of opening interoperability to such potentially unreliable providers (despite their best intentions), is not worth the privacy and security risks involved.

2.1.3. Interoperability in the legislative proposals

The EU Digital Markets Act

The original DMA proposal contained several provisions that broadly construe interoperability as applying only to 'gatekeepers'—i.e., the largest online platforms:

1. Mandated interoperability of 'ancillary services' (Art 6(1)(f));
2. Real-time data portability (Art 6(1)(h)); and
3. Business-user access to their own and end-user data (Art 6(1)(i)).

The first provision, (Art 6(1)(f)), is meant to force gatekeepers to allow users to access third-party payment or identification services—for example, to allow people to create social media accounts without providing an email address, which is possible using services like 'Sign in with Apple.' This kind of interoperability does not pose as big of a privacy risk as

mandated interoperability of 'core' services (e.g., messaging on a platform like WhatsApp or Signal), partially due to a more limited scope of data that needs to be exchanged.

However, even here, there may be some risks. For example, users may choose poorly secured identification services and thus become victims of attacks. Therefore, it is important that gatekeepers not be prevented from protecting their users adequately. The new drafts of the DMA adopted by the European Council and by the European Parliament attempt to address that, but they only allow gatekeepers to do what is 'strictly necessary' (Council) or 'indispensable' (Parliament).[29] This standard may be too high and push gatekeepers to offer lower security to avoid liability for adopting measures that would be judged by EU institutions and the Courts as going beyond what is strictly necessary or indispensable.

The European Parliament's draft goes significantly beyond the original proposal mandating interoperability of 'number independent interpersonal communication services' (letter (fa)) and of social network services (letter (fb)). In both cases, the provisions state that

> Interconnection shall be provided under objectively the same conditions and quality that are available or used by the gatekeeper, its subsidiaries or its partners, thus allowing for a functional interaction with these services, while guaranteeing a high level of security and personal data protection.

Moreover, Parliament envisages that the European Commission will prepare a specification for interoperability of social network services.

[29] European Council, General Approach to the Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) 2020/0374(COD), 16 November 2021, 13801/21; Amendments adopted by the European Parliament on 15 December 2021 on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9- 0419/2020 – 2020/0374(COD)), P9_TA(2021)0499.

Those provisions are good examples of overly broad and irresponsible interoperability mandates. They would cover 'any providers' wanting to interconnect with gatekeepers, without adequate vetting (unlike in Open Banking). The safeguard proviso mentioning 'high level of security and personal data protection' does not come close to addressing the seriousness of the risks created by the mandate. Instead of facing up to the risks and ensuring that the mandate itself is limited in ways that minimize them, the proposal seems just to expect that the gatekeepers can solve the problems if they only 'nerd harder'.

The other two provisions do not mandate full two-way interoperability, where a third party could both read data from a service like Facebook and modify content on that service. Instead, they provide for one-way 'continuous and real-time' access to data—read-only.

The second provision (Art 6(1)(h)) mandates that gatekeepers give users effective 'continuous and real-time' access to data 'generated through' their activity. It's not entirely clear whether this provision would be satisfied by, e.g., Facebook's Graph API, but it likely would not be satisfied simply by being able to download one's Facebook data, as that is not 'continuous and real-time.'

Importantly, the proposed provision explicitly references the General Data Protection Regulation (GDPR), which suggests that—at least as regards personal data—the scope of this portability mandate is not meant to be broader than that from Article 20 GDPR. Given the GDPR reference and the qualification that it applies to data 'generated through' the user's activity, this mandate would not include data generated by other users—which is welcome, but likely will not satisfy the proponents of stronger interoperability.

The third provision from Art 6(1)(i) mandates only 'continuous and real-time' data access and only as regards data 'provided for or generated in the context of the use of the relevant core platform services' by business users and by 'the end users engaging with the products

or services provided by those business users.' This provision is also explicitly qualified with respect to personal data, which are to be shared after GDPR-like user consent and 'only where directly connected with the use effectuated by the end user in respect of' the business user's service. The provision should thus not be a tool for a new Cambridge Analytica to siphon data on users who interact with some Facebook page or app and their unwitting contacts.

The bills in the US Congress

All US bills considered here introduce some interoperability mandates and none of them do so in a way that would effectively safeguard information privacy and security.

Rep. Cicilline's 'American Choice and Innovation Online Act' (ACIOA) would make it unlawful (in Section 2(b)(1)) to:

> restrict or impede the capacity of a business user to access or interoperate with the same platform, operating system, hardware and software features that are available to the covered platform operator's own products, services, or lines of business.

The language of the prohibition in Sen. Klobuchar's 'American Innovation and Choice Online Act' (AICOA) is similar (also in Section 2(b)(1)). It forbids covered firms from

> materially restrict[ing] or imped[ing] the capacity of a business user to access or interoperate with the same platform, operating system, hardware or software features that are available to the covered platform operator's own products, services, or lines of business that compete or would compete with products or services offered by business users on the covered platform.

Both ACIOA and AICOA allow for affirmative defenses that a service provider could use if sued under the statute. Even though those defenses mention privacy and security they are narrow ('narrowly tailored, could not be achieved through a less discriminatory means, was nonpretextual, and was necessary') and would not prevent service providers from incurring significant litigation costs. Hence, just like the provisions of the DMA, they would heavily incentivise covered service providers not to adopt the most effective protections of privacy and security.

Finally, Rep. Scanlon's 'Augmenting Compatibility and Competition by Enabling Service Switching Act' (ACCESS) would mandate that (in Section 4(a)):

> A covered platform shall maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to facilitate and maintain interoperability with a competing business or a potential competing business that complies with the standards issued pursuant to section 6(c).

The bill seems to place the burden of ensuring privacy of shared user data on third-party providers accessing the first provider's interface, while failing to address the question of foreign bad actors who might not be deterred by any threat of civil (or even criminal) action in the US, but could still benefit from the bill in accessing data. Nevertheless, the bill does state in Section 4(d) that

> a covered platform shall set privacy and security standards for access by competing businesses or potential competing businesses to the extent reasonably necessary to address a threat to the covered platform or user data.

This language is not much more permissive for privacy-securing actions of covered service providers than in the case of the other bills discussed here. Hence, just like those other

provisions it shows a policy choice to favour uncertain and speculative competition gains over clear and present danger to privacy.

One feature that negatively distinguishes Rep. Scanlon's ACCESS bill is the following provision (Section 4(e)(1)):

> A covered platform may make a change that may affect its interoperability interface by petitioning the [Federal Trade] Commission to approve a proposed change (…)

In other words, the bill would require many software updates, including security updates, to be vetted by the Federal Trade Commission before they are implemented. As noted by commentators, this is 'anathema to the structure that has been adopted and advocated by security experts'.[30] The bill does have an exemption for some security updates, but this exemption includes the familiar narrow language, which – even when applicable – will add friction (e.g. requiring involving in-house lawyers to decide whether a particular system update meets the narrow exemption or whether it has to be submitted to the Federal Trade Commission).[31]

Given the breadth of the interoperability mandates in the discussed US bills even compared to the DMA, they are likely to cover the issue of sideloading, which the DMA treats separately and which I discuss in the next subsection.

[30] Tatyana Bolton, 'Security in antitrust: implications of two house bills' (RStreet Institute, November 2021) https://www.rstreet.org/wp-content/uploads/2021/11/explainer32.pdf. See also Masnick, 'Will Congress' Big New Push…'.

[31] Section 4(e)(2): 'A covered platform may make a change affecting its interoperability interfaces without receiving approval from the Commission if that change is necessary to address a security vulnerability or other exigent circumstance that creates an imminent risk to user privacy or security if the change is narrowly tailored to the vulnerability and does not have the purpose or effect of unreasonably denying access or undermining interoperability for competing businesses or potential competing businesses.'

2.2. Device neutrality (sideloading)

The EU Digital Markets Act contains specific provisions, in Article 6(1)(c), about sideloading, i.e. allowing installation of third-party software through alternative app stores other than the one provided by the manufacturer (e.g. Apple App Store for iOS devices). A similar express provision for sideloading is included in Sen. Blumenthal's Open App Markets Act (Section 3(d)(2)). Moreover, the broad interoperability provisions in the other US bills discussed above may be interpreted as also requiring sideloading.

The motivation behind this provision seems, at least partially, to come from hacker mentality. Power users, hackers, tinkerers, are frustrated by being prevented from controlling and modifying all aspects of devices they own. This is understandable, but a myopic focus on expert users fails to address the point I made earlier that privacy and security affecting laws should be drafted with ordinary users in mind. The question is then, how will ordinary, non-expert users be affected by a sideloading mandate.

A sideloading mandate aims to give users more choice but can only achieve this by taking away from them the option of choosing a device with a 'walled garden' approach to privacy and security (such as is taken by Apple with iOS). The walled garden approach can be compared to Odysseus' choice to tie himself to a mast to prevent himself from acting in ways that could hurt him. Odysseus' choice may be inimical to the hacker or tinkerer mentality, but it can be perfectly rational for other users and the proponents of sideloading mandates have not so far established otherwise.

By taking away the choice of a walled garden environment, a sideloading mandate will effectively *force* users to use whatever alternative app stores are preferred by the developers of the applications users want to use. As Marco Arment noted

> Facebook owns four of the top ten apps in the world. If side-loading became possible, Facebook could remove Instagram, WhatsApp, the Facebook app, and Messenger from Apple's App Store, requiring customers to install these extremely popular apps directly from Facebook via side-loading. And everyone would. (...)
>
> Technical limitations of the OS would prevent the most egregious abuses, but there's a *lot* they could still do. We don't need to do much imagining — they already *have* attempted multiple hacks, workarounds, privacy invasions, and other unscrupulous and technically invasive behavior with their apps over time to surveil user behavior outside of their app and stay running longer in the background than users intend or expect.[32]

Other developers will have strong incentives to set up their own app stores or to move their apps to app stores with the least friction (for developers, not users) – which would also mean the least privacy and security scrutiny. This is not to say that Apple's app scrutiny is perfect, but it is reasonable for an ordinary user to prefer Apple's approach because it provides greater security.[33] Thus, a legislative choice to override the revealed preference of millions of users for a "walled garden" approach should not be made lightly.

The DMA's sideloading provisions, as amended by the European Council and by the European Parliament, contain what is intended as a safeguard proviso:

> *Council:* The gatekeeper shall furthermore not be prevented from taking to the extent strictly necessary and proportionate measures enabling end users to protect security in relation to third party software applications or software application stores. (Council)

[32] Marco Arment, 'The future of the App Store' (Marco.org, 13 September 2021) https://marco.org/2021/09/13/future-of-the-app-store.
[33] See also NOKIA, 'NOKIA Threat Intelligence Report 2020', https://www.nokia.com/networks/portfolio/cyber-security/threat-intelligence-report-2020/; Randal C. Picker, 'Security Competition and App Stores' (Concurrentialiste: Journal of Antitrust Law, 23August 2021) https://leconcurrentialiste.com/picker-app-stores/.

Parliament: The gatekeeper shall not be prevented from taking measures that are both necessary and proportionate to ensure that third party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper or undermine end-user data protection or cyber security provided that such necessary and proportionate measures are duly justified by the gatekeeper.

Sen. Blumenthal's Open App Markets Act includes similar narrow exempting provisions in its Section 4.

Besides the familiar problem of narrowness of such privacy safeguards, there is a more general issue: the core of the sideloading mandate prohibits outright an entire privacy and security-protection model. A model that many users are rationally choosing today. Even with broader exemptions this loss will be genuine and it is unclear whether taking away this choice from users is justified.

2.3. Compulsory data access for research or investigations[34]

Increasing transparency about the inner workings of 'very large online platforms' ('VLOPs') is among the main regulatory tools that the EU Digital Services Act ('DSA') envisages for VLOPs.[35]

A serious problem with information and transparency obligations is that if service providers are required to disclose too much about their moderation and security practices, they will be in effect providing guidelines to bad actors (terrorism promoters, spammers and other

[34] This section builds on my previous working paper 'The Digital Services Act: Assessment and Recommendations' (July 2021), https://ssrn.com/abstract=3874961.
[35] VLOPs are defined in Article 25 DSA as online platforms which provide 'services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million'.

criminals) on how to evade the safeguards. It is desirable for providers to supply a certain level of clarity to users on what content may be removed, but this needs to be weighed against the risks.

One way in which this risk may be managed is through non-public privileged access to information for vetted researchers and for authorities, which the DSA introduces in Article 31. However, access for researchers and for authorities nonetheless comes with serious risks to privacy, data protection and to commercial secrets.[36] Once the data from a digital service provider is exfiltrated to an external body or once researchers are given remote access to such data, a new surface of attack is opened for any interested party, including both criminals and intelligence services of unfriendly countries.

This new surface of attack is likely to be much easier for hackers to exploit than the systems of at least the major digital service providers are today. The exceptionally high level of internal security measures protecting the databases of at least some major online platforms is extremely unlikely to be matched by academic researchers or even by public authorities other than specialised military units and intelligence agencies.[37]

This is not just an issue of protecting personal data and commercial secrecy — protection of databases of online platforms is also a national security issue. Many public servants and others in positions of responsibility use public online platforms for communication, hence any access to such platforms' databases risks exposing highly sensitive data of those persons.

---

[36] Amnesty International (2021) 'Amnesty International Position on the Proposal for a Digital Services Act and a Digital Markets Act' (https://www.amnesty.eu/news/amnesty-international-position-on-the-proposals-for-a-digital-services-act-and-a-digital-markets-act/) 14; DOT Europe (2021) 'A Single Market for Digital Services: DOT Europe Questions and Recommendations on the DSA' (https://doteurope.eu/wp-content/uploads/2021/04/DOT-Europe-DSA-Questions-and-Recommendations-Chapters-1-3-.pdf) 26.

[37] It is not difficult to find examples of breaches of government systems, like the 2016 breach of the Office of Personnel Management, see e.g. Michael Adams (Lawfare, 11 March 2016) 'Why the OPM Hack Is Far Worse Than You Imagine' https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

Article 31(1) DSA establishes a power for national public authorities ('Digital Services Coordinators') and for the European Commission to request 'access to data that are necessary to monitor and assess compliance with' the DSA. Article 31(2) DSA allows 'vetted researchers' to request access, but their requests would have to be mediated by public authorities and can only be for the purpose of studying 'systemic risks' associated with a VLOP's activity.

The DSA recognizes the privacy and security risks associated with data access and allows service providers to object to a data access request on the grounds that 'giving access to the data will lead to significant vulnerabilities for the security of its service or the protection of confidential information' (Article 31(6)(b)). However, this objection may be overruled by the relevant public authority (Article 31(7)). Moreover, the vetted researchers must be able to 'preserve the specific data security and confidentiality requirements corresponding to each request' (Article 31(4)). What are the security and confidentiality requirements? The DSA provides that the detailed requirements are to be determined later in delegated legislation (Article 31(5)).

It is possible that the delegated legislation will take seriously the risks involved and adopt an approach along the lines I suggest below.[38] However, it is also possible that such risks will be discarded as mere special pleading from service providers. Given that the details of those requirements will decide whether the data access regime becomes a major threat to security and privacy, leaving so much to delegated legislation is irresponsible.

The law should leave no doubt that neither public authorities nor academic researchers can request direct access to full (live, production) databases of online platforms. In such a

[38] See also Mathias Vermeulen, 'The Keys to the Kingdom' (Knight First Amendment Institute, 27 July 2021) https://knightcolumbia.org/content/the-keys-to-the-kingdom.

situation public authorities and academics could not satisfy the requirement to 'preserve the specific data security and confidentiality requirements' (Article 31(4)).

The DSA should explicitly state that Article 31 access would not involve direct access to 'live' ('production') databases, but at most access to curated proxy databases. Such proxy databases will need to be sanitized (anonymised, e.g. using differential privacy techniques), for example in relation to personal and sensitive data.

However, preparing such proxy databases may prove to be costly and difficult even for the largest platforms. The DSA should provide a mechanism to assess the proportionality of the cost of each data access request to the benefit that it will bring. The original proposal did not provide for such proportionality assessment explicitly,[39] but the version adopted by the European Council does.[40]

Despite such measures, given the potential sensitivity of the data — in part, because it can be used to circumvent the moderation and security safeguards of online platforms — there should be a proportionate vetting process for anyone who may have access to the data, including not only the researchers but all individuals with access (e.g. administrative access) to systems or networks from which the data may be extracted (at least in an unencrypted form). The criteria provided in Article 31(4) do not address the seriousness of the issue.

[39] The proposal provided only, in Article 31(5) that the delegated legislation 'laying down the technical conditions under which very large online platforms are to share data' should take 'into account the rights and interests of the very large online platforms and the recipients of the service concerned. It is not entirely clear whether the issue of proportionality of cost to potential benefits would be covered by this provision – the Council's proposal makes this much more explicit (see the footnote below).

[40] The Council's new Article 31(4)(d) adds a requirement that 'the application submitted by the researchers justifies the necessity and proportionality for the purpose of their research of the data requested and the timeframes within which they request access to the data, and they demonstrate the contribution of the expected research results to the purposes laid down in paragraph 2'.

Even though the DSA says that detailed rules on how data access would work must take into account the interests of 'the recipients of the service', there is a risk that the interests of users will not be adequately safeguarded in the future rule-making process. Moreover, the users —whose data will be potentially at risk—will have no say in the process of data access under the Article 31 process. Only the provider of the online platform will be able to request amendments of a data access request. But it should not be expected that the provider will have sufficient motivation or resources to make the case for the protection of user interests, as distinguished from the provider's own interests. Moreover, it will be the public authority of the country where the provider of the online platform is established who will decide whether to grant a data access request. Such public authority may lack knowledge or motivation to adequately consider the interests of at least some categories of users of the platform.[41]

3. Conclusions

All of the legislative proposals considered here, both from the EU and from the US, betray a policy preference of privileging uncertain and speculative competition gains at the expense of introducing a new and clear danger to information privacy and security. The proponents of those or even stronger legislative interventions seem much more concerned, for example, that privacy safeguards are 'not abused by Apple and Google to protect their respective app store monopoly in the guise of user security.'[42] However, given the

[41] See also Mikołaj Barczentewicz, 'The Digital Services Act and Small and Medium Enterprises as users of online services' (EPICENTER policy brief, 13 October 2021) http://www.epicenternetwork.eu/research/briefings/the-dsa-and-small-and-medium-enterprises-as-users-of-online-services/.

[42] Damien Geradin, 'Digital Markets Act (DMA): Where is the Council Headed to?' (The Platform Law Blog, 18 October 2021) https://theplatformlaw.blog/2021/10/18/digital-markets-act-dma-where-is-the-council-headed-to/.

problems with ensuring effective enforcement of privacy protections (especially in respect to actors coming from outside of the EU, the US and other broadly privacy-respecting jurisdictions), the lip-service paid by the legislative proposals to privacy and security is not much more than that. A much more detailed vision of concrete safeguards and mechanisms of enforcement should be expected from policymakers proposing rules that come with entirely predictable and very significant privacy and security risks. Such vision is lacking on both sides of the Atlantic, and the hand-waving solution of legislating that the service providers are somehow to solve a problem to be created by the law is irresponsible.

I do not want to suggest that interoperability is undesirable. The argument of this paper was focused on *legally mandated* interoperability. Firms experiment with interoperability all the time — the prevalence of open APIs on the Internet is a testament to this. My aim, however, is to highlight that interoperability is complex and exposes firms and their users to potentially large-scale cyber vulnerabilities. Law makers imposing generalized obligations on firms to open their data, or create service interoperability short-circuit the private ordering processes that seek out the forms of interoperability and sharing that pass a cost-benefit test. The result will likely be both over inclusive and underinclusive. It would be overinclusive by requiring all firms that are in the regulated class to broadly open their services and data to all interested, even where it wouldn't make sense for privacy, security, or other efficiency reasons. It is underinclusive because the broad mandate will necessarily sap the resources of the regulated firms and deter them from looking for new innovative uses that *might* make sense but that are outside of the broad mandate. Thus, the likely result is less security and privacy, more expense, and less innovation.