Before the

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

In the Matter of International Internet Policy Priorities	)))))	Docket No. 180124068–8068–01

COMMENTS OF TECHFREEDOM

Scott Delacourt
Megan Brown
Joan Stewart
Kathleen Scott
WILEY REIN LLP
1776 K Street NW
Washington, DC 20009

Berin Szoka, President
James Dunstan, General Counsel
Ashkhen Kazaryan, Legal Fellow
TECHFREEDOM
110 Maryland Ave NE, Suite #409
Washington, DC 20002

July 17, 2018

TABLE OF CONTENTS

I. INTRODUCTION 1

II. THE UNITED STATES MUST CHAMPION A CLEAR U.S. ALTERNATIVE TO THE GLOBAL PRIVACY AND SECURITY TRENDS THREATENING THE OPEN INTERNET. 4

III. THE GDPR IMPEDES THE FREE FLOW OF INFORMATION, CONSTRAINING INNOVATION, ECONOMIC GROWTH, AND FREE EXPRESSION. 7

A. By Over-Penalizing Violations, the GDPR Chills Innovation and Risk Taking. 11

B. The GDPR Undermines Free Business Content Models and Constrains the Quality of Modern Internet Services. 13

C. GDPR's "One-Size-Fits-All" Approach Diverts Resources to Low-Utility Compliance at the Expense of Capital Investment. 17

IV. NTIA SHOULD ENSURE A PROCESS THAT IS TRANSPARENT AND COLLABORATIVE FOR DEVELOPING AND ARTICULATING ANY U.S. ALTERNATIVE TO THE GDPR. 19

V. CONCLUSION 20

I. INTRODUCTION

TechFreedom is a non-profit, non-partisan technology think tank focusing on issues of Internet freedom and technological progress while working to protect innovation and discovery. Technology is the great driver of social progress and human well-being, and we aim to keep it that way. We welcome this opportunity to provide information to the National Telecommunications and Information Administration ("NTIA") regarding its international Internet policy, including privacy and security questions that affect Internet openness and growth. In line with our mission, we urge NTIA to champion and continue to defend the free, open, and borderless Internet.

For over two decades, the Internet has flourished as the globally interconnected and interoperable network of networks: absent outright censorship, users have been able to connect with other users anywhere in the world. But now, the free, open, and borderless Internet is at risk of balkanization because of privacy and security regulations. Some jurisdictions are turning away from an open and liberalized approach to technology regulation, and instead are emphasizing political borders, burdensome regulation, and protectionist trade policies that would extend far beyond their borders. The most pressing example of an overly burdensome regulation that threatens the free flow of information is the European Union's General Data Protection Regulation ("GDPR").[1] The GDPR represents a fundamentally different approach to privacy, inverting the data ownership model that has characterized Internet development to date. While recent discussions about GDPR have focused on the cultural and moral underpinnings of Europe's approach, as companies in the United States and around the world work to come into

[1] Commission Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 ("GDPR").

compliance and avoid crushing penalties and vague, open-ended legal liability, the impacts on innovation, commerce, and free expression will be substantial.

As NTIA considers federal policy in these important areas, it must ensure that the Internet remains free, open, borderless *and innovative.* That means *both* (a) ensuring the continued flow of data, and interoperability of Internet services, across borders *and* (b) defending the freedom of American citizens and businesses to continue doing what has made the Internet great: experimenting and innovating without having to seek permission, or having to build an elaborate compliance infrastructure for a startup, first. Yes, the U.S. government must respect the sovereignty of nations to pursue their own domestic policies, but as an independent sovereign, the United States has an interest in clarifying and limiting the impact of overseas regulations, like the GDPR, to the extent they threaten to stifle innovation, stifle competition, curb economic growth, and restrict free expression by impeding the free flow of information. The U.S. government should be wary of calls for harmonization predicated upon acceptance of the underlying pro-regulatory approach that some countries and regions are taking.[2] The U.S. government must lead in defending a free, open, borderless, and innovative Internet—just as American companies have led in actually building such services.

The U.S. government interest is particularly pronounced where extraterritorial effects of overseas regulations directly impact U.S. industry, as with the GDPR. The United States should respect the European privacy approach, but confidently champion its own, equally valid

[2] *See* Alan McQuinn & Daniel Castro, *Why Stronger Privacy Regulations Do Not Spur Increased Internet Use*, Information Technology & Innovation Foundation (July 11, 2018), https://itif.org/publications/2018/07/11/why-stronger-privacy-regulations-do-not-spur-increased-internet-use?mc_cid=6ef5636fad&mc_eid=ff7c0376f1 ("[T]here is little evidence to suggest that beyond some minimum baseline of consumer protection, stronger privacy regulations increase trust, adoption, or use. On the contrary, additional regulation restricts the supply of digital technologies by raising costs and reducing revenues for companies to invest in new products and services. In short, the conventional wisdom about the connection between regulation and trust is wrong. Policymakers should reject proposals purporting to increase trust through greater regulation of the digital economy if they come at the expense of innovation and consumer welfare.").

approach that protects consumer privacy while balancing other essential interests. Most importantly, the U.S. government should make clear that in the U.S. system, innovation, economic growth, and free expression are paramount consumer interests—and that these interests can be protected while also addressing real privacy risks. It should explain that regulation should be a last resort because it can stymie innovation and distort markets by favoring incumbents and large organizations capable of managing compliance costs and navigating vague but staggering potential legal liability. Indeed, consumers all over the world have overwhelmingly benefited from America's minimally-restrictive, free-market regime, which has allowed for innovation, economic growth, and free expression while protecting against clearly articulated consumer harms.

For too long, some observers have attributed to the United States a policy of inattention to privacy and security because there is no single overarching, prescriptive "comprehensive" regulatory superstructure they can read. This is a misunderstanding of the U.S. approach to consumer protection. Articulating key policy principles may provide a better sense of the existing U.S. sectoral approach to privacy; this should be NTIA's top priority. In the *International Internet Policy Priorities Notice of Inquiry* ("*NOI*"),[3] NTIA rightly notes that the United States has long promoted "smart and nondiscriminatory privacy rules" and that "different approaches to protecting citizens' privacy, …. need not impede global commerce."[4] NTIA is well-positioned to emphasize the harmful effects of the surreptitious export of domestic regulatory policies; to champion the American approach to privacy, which protects consumer privacy alongside other important consumer interests in an innovative free-market economy; and

[3] *International Internet Policy Priorities*, Notice of Inquiry, NTIA Docket No. 180124068-8068-01, 83 Fed. Reg. 26036 (June 5, 2018) ("NOI").
[4] *Id.* at 26037.

to defend U.S. enterprise from regulation and punishment by other governments. NTIA is also well-positioned to develop and articulate the U.S. alternative to the GDPR in a transparent and collaborative way. Indeed, the process through which NTIA responds to international threats to the Open Internet will be no less important than the output.

II. THE UNITED STATES MUST CHAMPION A CLEAR U.S. ALTERNATIVE TO THE GLOBAL PRIVACY AND SECURITY TRENDS THREATENING THE OPEN INTERNET.

NTIA's NOI demonstrates a healthy concern for consumer welfare and the economic benefits that flow from the free, open, and borderless Internet. It asks about "challenges to the free flow of information online" and "the impact on U.S. companies and users."[5] NTIA need not look far to identify impending threats to digital citizens and to the Open Internet—which include threats to innovation, global commerce, and free expression—from burgeoning regulation of the digital economy. Privacy and security regulations are proliferating in Europe, South America, and Asia. Gathering threats include forced data localization,[6] certification regimes[7] that can act as barriers to entry, prescriptive security rules,[8] and heavy-handed regulation of international data flows and uses, such as the GDPR.[9] As the U.S. Chamber of Commerce recently explained:

---

[5] NOI at 26038.

[6] William Allen Reinsch, Center for Strategic & International Studies: The Future of Digital Trade Policy & the Role of the U.S. & UK, *A Data Localization Free-for-All?* (March 9, 2018), https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all ("China requires that "important data" concerning Chinese citizens be stored and processed locally. This data localization law allows China to restrict market access for cloud computing if the required data localization requirements are not met. The Chinese law also stipulates data localization requirements for the financial services industry and for telecommunications." "Russia's strict data localization policies also impact business decisions.")

[7] Under a European Commission (EC) Cybersecurity Act, the EC would establish rules to create certification schemes for Internet-connected devices and services.

[8] The Directive on the security of networks and information systems (known as the NIS Directive) promotes the "standardisation of security requirements …To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards so as to ensure a high level of security of network and information systems at Union level." Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (66).

[9] Other countries are considering and adopting GDPR-type data regulations. For example, Brazil's General Data Protection Regulation ("LGPD") has just been approved by that country's legislature. *See* Direu Santa Rosa,

> [f]or the past few decades, the dominant narrative in global policy debates was largely built on the twin pillars of promoting competition and increasing liberalization across industries, including in the telecoms and internet sectors. This paradigm was deregulatory in nature and saw protectionist policy as inherently undesirable and the free flow of information and capital as values to be promoted. This was critically important for the growth and success of the internet. A different outlook is developing in some parts of the world.[10]

A retreat from economic freedom and light-touch regulation of the Internet now threatens to impose unnecessary and undemocratic burdens on companies and citizens around the world. New rules can act as a drag on productivity everywhere. Notably, "increased costs raise barriers to market entry for would-be startups, repressing innovation and reducing an economy's competitiveness in the long term."[11]

Unnecessarily prescriptive Internet regulation also harms users by altering, or breaking, the business models that have allowed the Internet economy to thrive. Countries pursuing Internet regulation do not only export their policy choices, they can "harm both the competitiveness of the country implementing the policies and other countries. Every time one country erects barriers to data flows, another country that relies on these data flows is also affected."[12] An escalation of barriers to the free flow of data—a digital, global trade war—will harm Internet users everywhere.

Development in the field of data protection in Brazil, IAPP (June 26, 2018), https://iapp.org/news/a/desarrollos-en-materia-de-proteccion-de-datos-en-brasil/; *Brazil's Senate Passes General Data Protection Law*, Hunton Andrews Kurth: Privacy & Information Security Law Blog (July 11, 2018), https://www.huntonprivacyblog.com/2018/07/11/brazils-senate-passes-general-data-protection-law/.

[10] U.S. Chamber of Commerce & Wiley Rein, *The IoT Revolution and Our Digital Security: Principles for IoT Security* (Sept. 2017), https://www.uschamber.com/IoT-security.

[11] Cody Ankeny, ITI, *The Costs of Data Localization* (Aug. 17, 2016) http://www.itic.org/news-events/techwonk-blog/the-costs-of-data-localization (citing various studies including by McKinsey Global Institute).

[12] Joshua P. Meltzer & Peter Lovelock, *Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia*, Brookings (Mar. 20, 2018), https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/.

Given that many of these regimes seem to target major U.S. companies, and sweep in U.S. organizations of all sizes,[13] we can expect that U.S. consumers will be harmed by rules into the development of which they have had no input and the ongoing implementation of which they cannot influence—except insofar as the U.S. government attempts to exercise its diplomatic influence, informed by this inquiry. The U.S. government should, at all times and to the fullest extent of its powers to do so, champion our values and protect U.S. economic interests from global regulation. NTIA should help the Administration develop and advance an approach to Internet policy that protects consumer privacy while promoting other important American values like innovation, economic growth, and free expression—values that will benefit Internet users worldwide, even if their own governments fail to recognize them or give them meaningful effect.

One timely example of the troubling retreat from Open Internet policies is the GDPR, discussed in detail below. While the GDPR has its underpinnings in legitimate cultural and philosophical trans-Atlantic differences with respect to privacy, the E.U.'s new regime also has blatantly mercantilist qualities that are antithetical to the free, open, and borderless Internet. In large part, it seems clear the "problem" the GDPR is designed to solve is the global dominance of leading U.S. Internet firms. It is no accident that the day the GDPR became effective, suit was immediately lodged against the leading U.S. Internet firms.[14] Ironically, however, while the GDPR will, no doubt, be successful in allowing European regulators to browbeat the leading American tech companies beloved by so many users around the world, extract billions in fines from them, and score political points in European media, we believe the GDPR will actually,

[13] "This new data protection law goes into force May 25, 2018 and will apply to all companies handling the consumer data of citizens within the European Union (EU), no matter the size, industry or country of origin of the business." Bret Piat, *What small business owners should know about GDPR and why*, CSO (May 2, 2018), https://www.csoonline.com/article/3269578/compliance/what-small-business-owners-should-know-about-gdpr-and-why.html.

[14] *See* Alex Hern, *Facebook and Google targeted as first GDPR complaints filed*, The Guardian (May 25, 2018), https://www.theguardian.com/technology/2018/may/25/facebook-google-gdpr-complaints-eu-consumer-rights.

ultimately harm startups and other smaller companies far more than it will harm today's biggest tech players.

Lessons from the GDPR can inform U.S. policy going forward as the U.S. and other countries formulate regulatory alternatives to GDPR.

III. THE GDPR IMPEDES THE FREE FLOW OF INFORMATION, CONSTRAINING INNOVATION, ECONOMIC GROWTH, AND FREE EXPRESSION.

Consumers benefit immensely from the progress spurred by a minimally-restrictive, liberalized, free-market economy.[15] Privacy is an important value, but "privacy" interests are not purely objective; they are varied, subjective, and situational.[16] Privacy values should not be seen to be in tension with innovation. Valid privacy interests can be advanced alongside consumers' interest in the Internet remaining free and open. The Open Internet yields innumerable benefits to consumers by enabling innovation, growth, and free expression. The free flow of information has been the driving force behind the U.S. approach to the Internet since its inception. Indeed, "[t]he Internet's unbridled success results from a minimal regulatory framework, which has been the foundation for the United States' global Internet leadership for decades."[17]

---

[15] Jeffrey Dorfman, *Ten Free Market Economic Reasons to be Thankful*, Forbes (Nov. 23, 2016), https://www.forbes.com/sites/jeffreydorfman/2016/11/23/ten-free-market-economic-reasons-to-be-thankful/#573119d96db7.

[16] Survey evidence reveals varied perspectives on "privacy." An individual's "concern rises and falls depending on the situation." Paul McNamara, *Pew Research finds more Americans value their privacy in the abstract than in reality* (May 20, 2015), https://www.networkworld.com/article/2924847/security0/pew-research-finds-more-americans-value-their-privacy-in-the-abstract-than-in-reality.html (describing Pew research results). KPMG conducted a survey that showed "What one consumer finds 'creepy'. . . [a]nother finds cool." *Companies that fail to see privacy as a business priority risk crossing the 'creepy line'*, KPMG (Nov. 6, 2016), https://home.kpmg.com/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-see-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html.

[17] Testimony of Mr. Tim Day before the H. Energy & Commerce Comm., Subcomm. on Digital Commerce & Consumer Protection hearing on Internet of Things Legislation, at 9 (May 22, 2018), https://docs.house.gov/meetings/IF/IF17/20180522/108341/HHRG-115-IF17-Wstate-DayT-20180522.pdf.

The GDPR blocks the free flow of information by limiting the business models and data use practices that have allowed useful, globally interoperable services to flourish and making certain privacy judgments and values paramount.[18] For example, while the GDPR recognizes, in principle, that information that can no longer be "attributed to a natural person" no longer requires the protections of the regulations,[19] it sets an exceedingly high bar in satisfying this anonymization standard—and fails to encourage data controllers to bother attempting to de-identify data. As Matt Wes explains, writing for the International Association of Privacy Professionals:

> anonymized data must be stripped of any identifiable information, making it impossible to derive insights on a discreet individual, even by the party that is responsible for the anonymization. When done properly, anonymization places the processing and storage of personal data outside the scope of the GDPR.
> The Article 29 Working Party has made it clear, though, that true data anonymization is an extremely high bar, and data controllers often fall short of actually anonymizing data.
> By contrast to anonymization, Article 4(5) of the GDPR defines pseudonymization as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information."
> …
> Whether pseudonymized data is "reasonably likely" to be re-identified is a question of fact that depends on a number of factors such as the technique used to pseudonymize the data, where the additional identifiable data is stored in relation to the de-identified data, and the likelihood that non-identifiable data elements may be used together to identify an individual.
> Unfortunately, the Article 29 Working Party has not yet released guidance on pseudonymization and what techniques may be appropriate to use. Additionally, because the GDPR does not go into effect until 2018, pseudonymization has not been the subject of enforcement actions by Data Protection Authorities. This puts data controllers who want to implement pseudonymization as an element of their GDPR compliance in a very difficult position.[20]

This legal uncertainty, which in turn serves to discourage de-identification of data, perhaps more than any other aspect of GDPR, reflects an elevation of theoretical privacy concerns

[18] GDPR, Article 1(2).

above practical concerns like cost—even while paying lip service to such concerns. Such an all-or-nothing, strict-liability approach is utterly incompatible with American privacy law—and, indeed, with the overwhelming consensus among privacy scholars that regulating data differently, depending on whether, and how effectively, it has been de-identified, will benefit users both by making possible beneficial uses of identified, aggregate data while also incentivizing companies not to retain data in identified form when they do not need to do so.

The effect of making theoretical privacy concerns paramount above all other interests is to subordinate a consumer's interest in a dynamic, free-market economy and its attendant benefits—including low-cost and abundant goods and services, employment opportunities, and a higher standard of living—to the detriment of consumer welfare. The GDPR acts as a hidden trade barrier that disrupts consumer access to and use of U.S. businesses. The effect is particularly pronounced with respect to global firms that serve large U.S. and European customer bases. Global GDPR compliance for these firms negatively impacts access to desired services for U.S. customers. Likewise, compliance costs will be passed on to U.S. consumers as free access is eroded and replaced with pay-to-play access.[19] The world's poorest Internet users, especially in the developing world, will suffer most. This, in turn, will harm American users by denying them the value of connecting with Internet users around the world — as individuals, content creators, entrepreneurs, and customers.

This dynamic is not limited to large firms. Even small firms (including non-profit organizations) with no physical presence in Europe and minimal European customers bases are

[19] Niam Yaraghi, *A case against the General Data Protection Regulation*, Brookings: Techtank Blog (June 11, 2018), https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-the-general-data-protection-regulation/ ("GDPR could increase the cost of the services that consumers are so used to receiving free of charge. In the pre-internet era, services cost actual money. With digitization, consumers are now able to pay for the services they receive with their private information rather than their money.").

compelled to comply with GDPR.[20] There are no true size limitations.[21] Such firms and organizations face the unenviable choice of incurring disproportionate compliance costs or curtailing the access to European customers. [22,23]

Likewise, the negative effects of GDPR will not be limited to traditional commercial activities. "Marketing" is not just companies selling shoes; it is the marketing of ideas, political agendas, and other things that, in the United States, enjoy the most heightened protection of the First Amendment. Already, with the GDPR, non-profits have struggled with compliance, with even the Internet Society—the world's largest trans-national organization representing Internet users—having implementation challenges.[24]

The outdated, mercantilist approach of the GDPR is a direct threat to the Open Internet, as it jeopardizes both consumers' abilities to use Internet services all over the world as they

---

[20] GDPR, Article 3; *See also GDPR Key Changes*, EUGDPR.org (last visited July 16, 2018), https://www.eugdpr.org/key-changes.html ("The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU."); *See also The GDPR's Reach: Material and Territorial Scope Under Articles 2 and 3*, Wiley Rein: Privacy in Focus (May 2017), https://www.wileyrein.com/newsroom-newsletters-item-May_2017_PIF-The_GDPRs_Reach-Material_and_Territorial_Scope_Under_Articles_2_and_3.html.

[21] GDPR, Article 30 (the GDPR provides a very limited exception for documentation obligations for certain companies with fewer than 250 people; however, these exceptions are so finely drawn that few companies qualify); *see also* Michael Baxter, *GDPR and the Small Business*, GDPR:Report (Jan. 9, 2018), available at https://gdpr.report/news/2018/01/09/gdpr-small-business/.

[22] Roslyn Layton, *Europe's Privacy and Net Neutrality Policies Kill Startups and Deter Consumers from Shopping Online*, Forbes (May 30, 2018), https://www.forbes.com/sites/roslynlayton/2018/05/30/europes-privacy-and-net-neutrality-policies-kill-startups-and-deter-consumers-from-shopping-online/#51b11dfd111a ("GDPR compliance costs companies millions of dollars, so many Americans firms have stopped serving the EU altogether. Europeans can no longer access online versions of the Chicago Tribune, the Los Angeles Times, New York Daily News, Orlando Sentinel, and Baltimore Sun."); *See also* Allison Schiff, *Verve Closes European Business Thanks to GDPR*, AdExchanger (Apr. 18, 2018), https://adexchanger.com/mobile/verve-closes-european-business-thanks-to-gdpr/ (discussing why mobile marketing program Verve had to shut down its European offices, including laying off employees).

[23] Matt Novak, *Dozens of American News Sites Blocked in Europe as GDPR Goes Into Effect Today*, Gizmodo (May 26, 2018), https://gizmodo.com/dozens-of-american-news-sites-blocked-in-europe-as-gdpr-1826319542.

[24] *FAQs: Opting in to the Internet Society's New Privacy Policy/GDPR*, The Internet Society (Apr. 2, 2018), https://www.sfbayisoc.org/2018/04/02/faqs-opting-in-to-the-internet-societys-new-privacy-policy-gdpr/ ("What if [I] miss the deadline? If you have not opted in to the Internet Society's new privacy policy by 25 May 2018, your membership will be canceled.").

migrate or travel and also to connect with other users all over the world. Specifically, as detailed below, the GDPR chills innovation and risk taking through draconian penalties, undermines free content business models and constrains the quality of modern Internet services, and diverts limited resources to low-utility compliance activities at the expense of capital investment. This will particularly hurt small businesses and, ironically, entrench the dominance of today's largest Internet companies.

A. By Over-Penalizing Violations, the GDPR Chills Innovation and Risk Taking.

While the United States has struggled with the question of defining cognizable harm in privacy cases and the question of "informational injury,"[25] the GDPR imposes draconian penalties, assuming—without any factual basis—massive harm from non-compliance. The GDPR imposes fines of 2-4% of a company's annual global revenue, or ten to twenty million Euros, whichever is higher, depending on the specific type of violation.[26] This approach assumes massive harm from privacy violations (which may turn on entirely theoretical harms) and makes the illogical and unsubstantiated leap that harm to consumers will scale in relation to a firm's revenues. Importantly, these fines are not intended to be returned to consumers as restitution for loss; instead, for the most part, they will go straight to the treasuries of European governments.[27] Consumers must separately pursue any action for compensation through the courts.[28] This is naked rent-seeking by the European Union, an attempt to tax American tech companies in the most undemocratic manner possible.

---

[25] *See, e.g.*, *Beck v. McDonald*, 848 F.3d 262, 273 (4th Cir. 2017) ("Our sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft."); *Informational Injury Workshop*, FTC (Dec. 12, 2017), https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop.
[26] *See* GDPR Article 83(4)-(5).
[27] *See* GDPR Article 83.1.
[28] *See* GCPR Article 82.

Additionally, the GDPR also pairs a private right of action[29] with a law whose requirements, while in full force and effect, remain very unclear. As one professor has characterized it, the GDPR is "a big, confusing mess."[30] The overall effect of the GDPR's indeterminate-but-potentially-enormous legal liability is to expose subject firms to a litigation lottery, and to transfer resources from productive economic activities, including innovation and risk taking, to rent-seekers who will use the process of litigation and political pressure to serve their own interests, not those of consumers—either American or European.

Translated to the U.S. context, the GDPR's private right of action would work far differently and have far more draconian effects. The realities of enforcement matter far more than the words on paper. Whereas the GDPR may intend a private right of action as a vehicle for an *individual* to seek enforcement of newly-created privacy rights, the U.S. system provides for relatively easy certification of *class actions*, which dramatically changes incentives and outcomes. Through the use—and abuse—of the class action form, relatively minor harms may be weaponized by a single individual, deemed a class representative and empowered to act on behalf of a larger group, to threaten massive damages, forcing strategic settlements from industry even where the likelihood of success in litigation is low. Moreover, lawyers specializing in class actions are the chief beneficiaries of such litigation, which routinely return trifling compensation to consumers—compensation so minimal they are often unclaimed by those purportedly injured—while delivering massive windfalls to lawyers.[31]

---

[29] *See* GDPR Article 79 ("[E]ach data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.").
[30] Alison Cool, *Europe's Data Protection Law Is a Big, Confusing Mess*, New York Times (May 15, 2018), https://www.nytimes.com/2018/05/15/opinion/gdpr-europe-data-protection.html (describing that "[n]o one understands G.D.P.R.," that it is "staggeringly complex," and that "the regulation is intentionally ambiguous").
[31] *See Engineered Liability: The Plaintiffs' Bar's Campaign to Expand Data Privacy and Security Litigation*, U.S. Chamber Institute for Legal Reform, at 22 (Apr. 2017),

Europe's enhanced privacy regulations and their accompanying draconian penalties will stifle innovation. The GDPR will entrench existing companies that can afford the compliance and litigation costs, effectively "freezing" the Internet as of 2018. Here, an analogy to the International Traffic in Arms Regulations ("ITAR") is instructive. In the ITAR context, the entire U.S. aerospace industry—including market structure and technologies—was frozen for almost two decades because only the large and incumbent aerospace companies could afford the compliance costs of having to treat *all* space technologies (which may or may not have had a dual use military potential) under the technology transfer controls designed for outright weapons. These costs were passed onto the government and commercial users. But far more significant than compliance costs were the overall effects on the ecosystem of consolidation and lost innovation. Only when ITAR restrictions were relaxed (and most space technologies were transferred from the ITAR's strict-liability regime to the Commerce Department's more flexible, risk-based export control regime for dual-use technologies) did we see the current rise of smaller, more agile companies that introduced new technologies, like small satellites.

B. The GDPR Undermines Free Business Content Models and Constrains the Quality of Modern Internet Services.

The free flow of information drives the modern Internet; indeed, it is this free flow that enables the "free" element of the "free and open Internet."[32] The Internet relies heavily on a free-content model that is supported by advertising. Leading U.S. Internet firms—along with a massive number of large, small, and mid-sized business that form a significant portion of the

https://www.instituteforlegalreform.com/uploads/sites/1/Engineered_Liability_The_Plaintiffs_Bars_Campaign_to_Expand_Data_Privacy_and_Security_Litigation.pdf ("The skyrocketing costs of contending with a data breach should not be exacerbated by opportunistic plaintiffs' lawyers who engineer liability claims for their own profit in the absence of real damage.").

[32] When we use the term "free and open Internet," of course, we mean both senses of the word "free," insofar as the freedom to experiment with business models allows some companies to experiment with free, generally ad-supported offerings while other companies experiment with payment-supported models.

robust and growing digital economy—base their business models, in whole or in part, on providing free content and services to consumers in exchange for access to their data for use in marketing. "Since the earliest days of the commercial web, online advertising has been a vital driver,"[33] and has "help[ed] [to] support diverse types of free content."[34] "Consumers get the benefits of the Internet at low cost, and often for free, because entrepreneurs are building out analytical tools and support services to run them leaner, and to create new revenue sources that let even free services be profitable."[35]

The exchange of consumer data for free content and services in the United States is *not* "unregulated." Rather, the Federal Trade Commission ("FTC"),[36] state Attorneys General, and private plaintiffs police such exchanges under a variety of authorities, including Section 5 of the FTC Act.[37] And consumers—both in the United States and Europe—overwhelming choose to share their information to receive the significant benefits of free or low-cost digital content and services.[38]

---

[33] *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, at 40 (May 2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf ("White House Big Data Report").

[34] *Improving the Consumer Online Ad Experience*, Coalition for Better Ads, https://www.betterads.org/research/.

[35] John Deighton &Leora D. Kornfeld, *Economic Value of the Advertising-Supported Internet Ecosystem*, Interactive Advertising Bureau, at 1 (Sept. 2012), http://www.iab.com/insights/economic-value-of-the-advertising-supported-internet-ecosystem/. ("IAB Ad-Supported Internet Study").

[36] The FTC Act serves as the basis for a notice and consent approach to privacy.

[37] 15 U.S.C. § 45(n).

[38] *See, e.g.*, Patricia A. Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, The Journal of Consumer Affairs (Mar. 6, 2007), *available at* https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1745-6606.2006.00070.x (detailing that "despite the complaints [about privacy rights and controlling personal data], it appears that consumers freely provide personal data"); *see also* Anindya Ghose, *When push comes to shove, how quickly will you give up your data for convenience?*, Quartz (May 2, 2017), https://qz.com/973578/data-privacy-doesnt-seem-to-be-a-concern-for-mobile-users-willing-to-swap-it-for-convenience/ ("[I]n one study conducted across 372 cities and towns in Germany, we involved the collaboration of 3,544 retailers, stores, and merchants. Firms uploaded coupons onto a mobile app, and by enabling their GPS feature and sharing their real-time location information, consumers were able to receive these deals. Consumer engagement rate of these location-based coupons exceeded that of other, more traditional mobile ads by a magnitude of three to 10 times.").

The free content model offers important benefits to consumers and the overall economy.[39] It reduces (or eliminates) the fees that consumers must pay for digital content and services, while at the same time "expand[ing] the size of the system that society can afford to have."[40] It also facilitates global interoperability, allowing people from around the globe — including the world's poorest people — to enjoy the benefits of the free flow of information and connect to the same global "network of networks" as far wealthier people in more developed countries. It creates jobs and contributes to the national economy.[41] It saves consumers time and other resources, and makes possible businesses that could not succeed otherwise, bringing consumers worldwide far more robust content and service offerings, and a degree of competition in providing both, that would be otherwise impossible.

The GDPR approach, however, undermines free content and service business models—and these models' attendant benefits—in a number of ways, including, but not limited to:

- Defining the class of data that is subject to regulation sweepingly in such a manner that processing of even innocuous data with little privacy significance triggers regulation;[42]

---

[39] *See* Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80-1 Antitrust L. J. 121, 130, (2015), https://www.ftc.gov/system/files/documents/public_statements/686541/ohlhausenokuliaralj.pdf ("Consumer data now forms the foundation of a wide variety of services, products, and business models, with enormous benefits to both competition and consumers.").

[40] IAB Ad-Supported Internet Study at 6.

[41] "The total global market [for Internet advertising] is expected to grow by a CAGR of 8.7% between 2017 and 2022 to reach a total value of US $339bn at the end of the forecast period," *see Global Entertainment & Media Outlook 2018-2022*, PwC (2017), *https://www.pwc.com/gx/en/industries/tmt/media/outlook/segment-findings.html*; while the U.S. Internet advertising "will rise at a 9.9% CAGR through 2021 and hit $116 billion in ad revenue by 2021, making it twice the size of the TV ad market." *PwC: Radio Ad Spend's Rise Comes Mainly From Digital*, InsideRadio (July 19, 2017), http://www.insideradio.com/free/pwc-radio-ad-spend-s-rise-comes-mainly-from-digital/article_969ea94c-6c52-11e7-91c5-fbfa07553c5d.html. *See also White House Big Data Report* at 40 ("One study estimated that the ad-supported Internet sustains millions of jobs in the United States and that the interactive marketing industry contributes billions to the U.S. economy each year.").

[42] *See* GDPR Article 4 (defining personal data to mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"); *see also* Kathleen Paisley, *It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, 41 Fordham Int'l L.J. 841 (May 2018),

- Compelling detailed notifications of data use in a manner that requires *a priori* determinations about how data will be used and limits flexibility to innovate while increasing liability exposure;[43]
- Enabling consumers to recapture or require the deletion of data after the agreed free content/services for data access exchange occurs;[44] and
- Requiring complex and detailed consent disclosures that will confuse and deter consumers, favoring traditional pay-for-service regimes that are not viable for many Internet businesses—and skewing the overall ecosystem in favor of the largest Internet companies.[45]

As an example of the effect of the GDPR on the free content and service model, one need look no further than Facebook. As Niam Yaraghi, of the Brookings Institution, writes:

> We can connect with our friends and family on Facebook without having to pay Facebook in dollars because instead we are paying Facebook with our private information, which then allows the social network to generate a source of revenue off it. By limiting the capability of Facebook to collect and use such data, GDPR effectively limits the ability of consumers to pay for such services with their private information. The obvious result is that Facebook has to either reduce its "free" services or start charging subscription fees in order to remain profitable.[46]

The free exchange of data also drives innovative new services, helps to improve existing services, and allows for the personalization and relevant content that modern digital citizens have come to demand and expect.[47] Just as consumers often choose to share their personal data in

https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2707&context=ilj (describing that under the "purposefully broad definitions of what constitutes both personal data and data processing," and even an activity like "shredding documents or taking notes" can be subject to the regulation).

[43] *See, e.g.*, GDPR Articles 12-14 (detailing the information that data controllers must provide to data subjects).

[44] *See* GDPR Article 17 ("The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay . . . .").

[45] *See, e.g.*, GDPR Article 12 (requiring data controllers to provide various information required under Articles 13-14, 15-22, and 34 "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" and requiring that the information be "provided in writing, or by other means, including, where appropriate, by electronic means").

[46] Niam Yaraghi, *A case against the General Data Protection Regulation*, Brookings: Techtank Blog (June 11, 2018), https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-the-general-data-protection-regulation/.

[47] *See Online Consumers Fed Up with Irrelevant Content on Favorite Websites, According to Janrain Study*, Janrain (July 31, 2013), https://www.janrain.com/company/newsroom/press-releases/online-consumers-fed-irrelevant-content-favorite-websites-according (showing that a large majority of online consumers—74%—get frustrated when advertising content is not personalized and "has nothing to do with their interests.").

return for free content, consumers also often choose to share their data for better, more personalized or relevant services and content.[48] Yaraghi continues:

> An obvious example is the relevance of the search results on Google. Without collecting extensive data on users and their preferences, Google will not be able to provide its users with tailored and highly relevant results every time they enter a search phrase. . . . A further example is Amazon's Alexa and Apple's Siri. These artificial intelligence inventions become smarter with the amount of data they collect and analyze; with limited collection and analysis of personal data, Alexa and Siri would be much less intelligent.[49]

With the advent of GDPR and other overly burdensome regulatory approaches that threaten to stifle the free flow of information, the goods and services that are synonymous with the modern digital world will become more expensive, if available at all. Innovations that could have been will not be — and that cost, perhaps the greatest cost of all, will go completely unseen. In short, in the name of privacy, the GDPR approach will harm consumers around the world.

C. GDPR's "One-Size-Fits-All" Approach Diverts Resources to Low-Utility Compliance at the Expense of Capital Investment.

The evolving U.S. privacy regime uses a sectoral approach tailored to the potential risks and harms arising from the data in question and its use by certain firms.[50] In addition, sectoral regimes often tailor regulation applicable to different industry players based on their size, ability to bear the cost of regulation, or intensity of data use.[51] By contrast, the GDPR uses a "one-size-

---

[48] *See* Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. Mo. B. 6, 76-77 (2016) (explaining that in the wearable technology market, "informed consumers have been willing to sacrifice a little privacy to gain the benefits associated with fitness trackers and smartwatches: improved wellness, vanquishing unhealthy eating habits, and feeling more liberated to manage their health care").

[49] Niam Yaraghi, *A case against the General Data Protection Regulation*, Brookings: Techtank Blog (June 11, 2018), https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-the-general-data-protection-regulation/.

[50] *See, e.g.*, HIPAA (regulating the privacy of health information); GLBA (regulating the privacy of financial information); CAN-SPAM (regulating privacy of email communications); Section 222 of the Communications Act (regulating privacy of specific information with regard to telecommunications carriers).

[51] For example, HIPAA's Security Rule lists the following factors to consider when determining an organization's security measures, allowing for flexibility: "(i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information." 45 C.F.R. § 164.306(b)(2)(i)-(iv).

fits-all" approach that heavily regulates all firms—including non-profits—controlling, processing and analyzing data, regardless of the risks arising from the particular data in question or its use. Moreover, there are no differentiations based on size or resources, "creating a class gap between the bigger and smaller companies" [52] and making GDPR an extremely regressive regulation, having a disproportionately burdensome effect on organizations with the fewest resources and the most limited ability to understand and implement it.

The impact of the GDPR's undifferentiated approach is to divert resources to compliance without regard to risk, with the effect of transferring resources from capital investment to low-utility compliance.[53] Encouraging a "greater focus on privacy," as the GDPR's defenders essentially argue, can in fact *reduce* effective privacy protection if it means diverting focus from serious privacy harms to theoretical harms and technical violations merely to avoid liability. While the second-order effects of GDPR are difficult to measure, the direct costs of compliance are beginning to become clear–and they are significant. Indeed, a survey by PwC of 300 top executives at companies in the United States, United Kingdom, and Japan found that among

[52] Dror Liwer, *Why mid-market companies face a tougher road with the GDPR*, CSO (May 1, 2018), https://www.csoonline.com/article/3269518/regulation/why-mid-market-companies-face-a-tougher-road-with-the-gdpr.html ("When a certain level of protection becomes mandatory it means that some players, the smaller ones, will be left out of the game . . . we are creating a class gap between the bigger and smaller companies.").

[53] Daniel Castro & Michael McLaughlin, *Why the GDPR Will Make Your Online Experiences Worse*, Fortune (May 23, 2018), http://fortune.com/2018/05/23/gdpr-compliant-privacy-facebook-google-analytics-policy-deadline/?mc_cid=675a472eec&mc_eid=3ee67fc4df ("The regulation places significant burdens on organizations. To comply with the GDPR's requirements, organizations have to buy and modify technology, create new data handling policies, and hire additional employees. For Fortune Global 500 companies, the biggest firms worldwide by revenue, the costs of compliance will amount to $7.8 billion. In the U.S., PwC surveyed 200 companies with more than 500 employees and found that 68% planned on spending between $1 and $10 million to meet the regulation's requirements. Another 9% planned to spend more than $10 million. With over 19,000 U.S. firms of this size, total GDPR compliance costs for this group could reach $150 billion. And this does not include smaller firms and nonprofit organizations, most of which, if they have European customers, will have their own compliance costs.").

those companies that had brought their operations into compliance, 88% spent more than $1 million and 40% had spent more than $10 million.[54]

IV. NTIA SHOULD ENSURE A PROCESS THAT IS TRANSPARENT AND COLLABORATIVE FOR DEVELOPING AND ARTICULATING ANY U.S. ALTERNATIVE TO THE GDPR.

The process by which NTIA develops and articulates the U.S. alternative to the GDPR is just as important as the output. Europe has demonstrated, through the GDPR, how to bypass the traditional collaborative approach to Internet policy-making on an issue of supreme importance through one conducted entirely by governments. As detailed above, that closed process produced overly burdensome policy that threatens the Open Internet.

The U.S. approach in developing any alternative to GDPR, led by NTIA, should be transparent and collaborative. There is a multiplicity of benefits that come from such an approach, not the least of which is that this approach allows government—which is inherently ill-suited to regulate emerging technologies—to better understand the benefits of innovative technologies. As TechFreedom has testified to Congress (about the 2012 Obama White House's proposed "Consumer Privacy Bill of Rights"):

> [D]eveloping the capacity to understand and effectively regulate technology is as much about ensuring that regulators understand how innovative technology confers benefits on consumers as it is about ensuring that regulators understand how new technology doesn't impose imaginary costs. As technological advance brings about ever more effective means of collecting and analyzing information, there is a tendency to view this through the lens of harm—to see such advances as ever more intrusive and potentially harmful. Forty years ago, the great economist Ronald Coase warned us: "If an economist finds something—a business practice of one sort or another—that he does not understand, he looks for a monopoly explanation. And as in this field we are very ignorant, the number of understandable practices tends to be very large, and the reliance on a monopoly

[54] *Pulse Survey: GDPR budgets top $10 million for 40% of surveyed companies*, PwC, https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html.

explanation, frequent."[55] The same risk arises here—that, finding a technology that they don't understand, regulators will look for a nefarious (or "unfair") explanation, overestimating harms to users (the more easily seen) and understating benefits (the more likely unseen).[56] Ensuring that regulators have the capacity to keep up with technological change is thus essential to facilitating both effective and appropriately restrained enforcement.[57]

V. CONCLUSION

The privacy approach adopted by the GDPR—which is a protectionist tool for European governments to hamstring U.S. companies in favor of their domestic counterparts—threatens the free and open Internet. By stifling the free flow of information, overly burdensome privacy regulations also stifle innovation, economic growth and the availability of valuable goods and services, and free expression. As the U.S. government interacts with its European counterparts and articulates any alternative to the GDPR—a process that should be open and transparent—the U.S. government should seek co-equal status for a different, but equally valid, privacy approach that more carefully balances consumer privacy interests with the overarching consumer interest in the open, free, borderless, and innovative Internet.

---

[55] Ronald Coase, *Industrial Organization: A Proposal for Research*, *in Economic Research: Retrospect and Prospect, 3 Policy Issues and Research Opportunities in Industrial Organization*, 59, 67 (Victor Fuchs ed. 1972).
[56] *See* Frédéric Bastiat, *What Is Seen and What Is Not Seen*, (Seymour Cain trans., George B. de Huszar ed., Foundation for Economic Education 1995), http://www.econlib.org/library/Bastiat/basEss1.html.
[57] Testimony of Berin Szoka before the H. Energy & Commerce Comm., Subcomm. on Commerce, Mfg., and Trade hearing on Balancing Privacy and Innovation, at 2-3 (Mar. 29, 2012), https://archives-energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/CMT/20120329/HHRG-112-IF17-WState-BSzoka-20120329.pdf.

Respectfully submitted,

/s/ Scott Delacourt
Scott Delacourt
Megan Brown
Joan Stewart
Kathleen Scott
WILEY REIN LLP
1776 K Street NW
Washington, DC 20009

/s/ Berin Szoka
Berin Szoka, President
James Dunstan, General Counsel
Ashkhen Kazaryan, Legal Fellow
TECHFREEDOM
110 Maryland Ave NE, Suite #409
Washington, DC 20002