AUTOMATTIC

November 9, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Attn: Privacy RFC
Washington, DC 20230
Submitted via email privacyrfc2018@ntia.doc.gov

Re: Docket No. 180821780– 8780–01, Comments from Automattic Inc.

Dear National Telecommunications and Information Administration:

Thank you for the opportunity to comment on the NTIA's proposed privacy approach.

We share your commitment to online privacy. It's a topic that we care deeply about at Automattic. Our users' privacy is critically important to us.

Let me first share more about Automattic. Automattic is a company with a singular mission: make the web a better place. All of Automattic's products and services are designed to democratize online publishing so that anyone with a story can tell it. Automattic is best known for WordPress.com. WordPress.com allows anyone, from large enterprises, to bloggers, plumbers, doctors and restaurant owners, to easily create a website on the web platform that powers more thoughts, musings, and businesses than any other in the world. WordPress.com is powered by WordPress – the world's most popular open source publishing software. The code behind WordPress is open-source, meaning that it is built by the WordPress community and can be downloaded, used, and modifyied, for free.

The proposed high level outcomes – especially those around transparency, control, choice, and openness – align very well with the things we care about at Automattic, and in the WordPress community.

Below we offer our perspective on the request for comments on how to achieve the desired privacy outcomes and goals–and in particular, how the United States can create create real, meaningful privacy protections for consumers through targeted rules that address the problems that pose the most risk to ordinary citizens.

Real Consumer Control with Data Portability

We won't have a truly open web, with real consumer control over their data, without giving consumers the ability to take their data with them to new services. That's why data portability must be featured as a desired outcome in the U.S. privacy framework. (*See Question A(1) Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items?)*

Automattic champions data portability. It's at the heart of our roots as an open-source company. We don't believe that software code or someone's data should be locked up behind closed, proprietary systems. That's terrible for the Internet, and at odds with the openness that allowed the Internet to grow into the greatest expressive medium of our time. For that reason, our users' content belongs to them, not to us. We hope users find our services useful, but if a user decides to move elsewhere, we provide them with all the tools to easily move their site and personal notes, without any extra charges from us.

What's more, data portability gives individuals *real* control over their online lives. Our data is not really "ours" when it's unreachable behind someone else's lock and key. Nor is our data "ours" when we have no ability to move our data to a new service that better fits our needs, or better protects our privacy, but the company we are stuck with can use our data for its analytics or marketing. To have meaningful control over their personal data, individuals must have the ability to easily take the data that they created within the context of an online service or app – in our world, that is site content and personal notes – to another service.

True Transparency

Transparency is the foundation of strong privacy protections. In order to make informed choices about the services they use, or the privacy options within a chosen service, a consumer must be able to understand what data is collected and how it is used.

The current U.S. privacy regime's directive that companies post full and complete privacy policies is a good thing. But with so much information available, transparency fatigue creeps in: Unable to read all of it, consumers read none of it.

Some may say that companies use privacy policies to hide and obfuscate their privacy practices, and perhaps that is true for some, but even an earnest company struggles to provide concise information in the face of the simple fact that not disclosing everything and anything could subject them to an FTC violation.

Here's how we suggest to bridge the gap between full disclosure and easily accessible disclosure: a "short list" of 5 types of data collection or use that must be highlighted at the top of any privacy policy. This short list should include the most high risk, most sensitive data collection, the very ones that consumers would most want to know about, such as precise location data for a mobile device, or targeted advertising based on sensitive data categories (political opinions,

race/ethnicity). To encourage companies to state these data practices/uses succinctly, and balance highlighted disclosure with full disclosure, there should be a "safe harbor" if more fulsome details are disclosed in the privacy policy itself.

An analogy already exists for highlighted disclosure, namely the Truth in Lending Act. Because of TIL, key terms like the interest rate, amount financed, and total of payments are featured at the top of loan documents. Applying a similar framework in the privacy context would likewise alert consumers of the data collections and use that would be of the most interest.

Targeted Rules and Choice Options for What Poses the Most Risk

We've shared a few of our ideas about how the United States can create actual, rather than theoretical, privacy protection for consumers. And we recognize that more can and should be done. But we caution against trying to tackle an ambiguous, large set of privacy concerns with one broad brush. To have meaningful privacy protections, we need clear rules that directly address the data practices that pose the most potential harm to consumers.

That means pinpointing what, exactly, most concerns us about online data practices–is it selling dossiers about individuals? Using sensitive information to profile individuals? Compiling data about an individual across multiple services for marketing? Sharing private data about people in ways that could have real, impactful consequences when they apply for a new job, or a new loan? And then we need to tailor laws to add meaningful consumer protections around the data practices that give us the most pause.

Identifying these risks is particularly important because even "tech" or "websites" are not all alike. Tech companies vary, and widely–in size, in their industry under the "tech" umbrella, and in what data that collect and how they use it. A social network, a publishing platform like WordPress.com, a search engine, an ad vendor, and an e-commerce business all have different needs and customer expectations when it comes to data. For example, Automattic is a small company of less than 800 total worldwide. Our business model is based on user loyalty and paid subscriptions to our products. Facebook has more than 50,000 employees, and an ads driven business model that touches vastly more personal data and information about the users of its platform. Both models pose different challenges, and involve different risks to consumers. The rules governing online privacy should take this into account.

What's more, today, because nearly every business has some online presence, privacy laws that are designed to apply to online business often sweep up even the smallest of operations. A grocery store loyalty program, a doctor's office, an airline, a gym, a local pizza parlor or church or community group–all these gather some form of information online. Trying to create abstract shared principals among all enterprises can lead quickly to confusion and unintended consequences without ever actually remedying the specifics risks to consumers.

Consider this: The GDPR has a set of rules that apply to "profiling"; that is, automated processing of personal data to evaluate certain things about an individual. Broadly speaking, a

company must be transparent about profiling, honor a user's right to object to that profiling, and run privacy impact assessments to determine how long to keep data, evaluate whether the use of the data is consistent with the purposes for which it was collected, weigh privacy interests and risks to the rights and freedoms of individuals, and evaluate appropriate security measures, among other considerations. The same rules apply whether you are a data broker, building up dossiers to sell about individuals based on their activity across websites, shopping store loyalty programs, financial information from house purchases, and the like, or whether you are a business simply tailoring your marketing to your existing customer base, about your own products, to make it most effective.

But *should* the rules be the same? The rules are often far too harsh for the sorts of targeted marketing that most companies use to make their marketing most effective. The rules also add a layer of burden that is too great for many companies. A midsized ecommerce store or tech company may have hold back on the very targeted marketing that it needs to compete with larger companies who have the resources (read: giant legal departments) to take care of all of these compliance obligations.

On the other hand, the rules may be far too light when it comes to more concerning data practices. For example, a dossier on someone built up across multiple services to target marketing deserves different privacy protections than an address used to target marketing to someone in a particular geographic area. Information about browsing history collected through cookies/pixels online and tied back to someone's name or email address for marketing should be treated differently than information tied to cookie ID 1234455699, and even more differently than analytics information collected through cookies/pixels about how visitors use a particular site in order to improve a site's performance. More sensitive data uses demand more transparency, more options for users, and more strictures on what companies can do with that data, regardless of whether it is disclosed in a privacy policy.

A gargantuan, omnibus privacy bill that shoots for the lowest common denominator across multiple products and services isn't going to give US consumers meaningful privacy protections. We encourage those crafting the US privacy framework to identify the specific types of data practices that trouble us, and then directly and specifically – not broadly and vaguely – target these worrisome data practices.

Let's give U.S. consumers real, tangible privacy protections.

Postscript: Talk to Small and Medium Sized Companies

The data practices of large technology companies drive discussions around privacy; but, any new privacy framework will equally – or better said, disproportionately – impact small and medium sized businesses, even though their data practices are far different. (*See Question C2. Should the Department convene people and organizations to further explore additional commercial data privacy-related issues? If so, what is the recommended focus and desired outcomes?*)

At Automattic we are, by comparison, a relatively small company, with less than 800 people and only 4 lawyers. Interpreting and implementing the requirements of GDPR took us months of work, involving dozens of people across the company, not to mention outside consultants, to work on compliance–even though we already had high privacy standards and are not in the business of selling personal data. As just one example, we, like most companies, updated our contracts with third party vendors who process personal data on our behalf. To accomplish that, we hired new staff, dedicated only to handling these paperwork updates. The cost of compliance can be heavy and real, not just for us, but for the many companies smaller than us that make up the internet.

More importantly, the GDPR was very difficult to understand for our customers, who are largely the small business owners and individuals who operate most of the world's web. An effective site is essential to them, and none of them have compliance departments. The fear and concern were deep for almost everyone we talked to in the U.S. And unfortunately there were often no simple, easy answers to offer, given how much in the GDPR is open to interpretation.

If every company is regulated like a huge international conglomerate, that may be all we have left in the end.

That's why you need the input of medium and small businesses who are the backbone of this country. Many of them are our customers. We expect you'll find that they, too, care very much about their own customers' privacy. It's core to the trust that any business – from an internet company to a main street retailer – builds with its customers. They just need a carefully crafted law that is clear and actionable for them, without an army of lawyers.

Here's what we suggest you ask small and medium business owners: What direction they need from any privacy framework in order to put solid privacy practices in place? What tools and support may be useful from the Small Business Administration? And how the U.S. privacy framework can target high risk data practices, without unintentionally burdening their routine data practices, and putting small and medium sized businesses at an unfair competitive disadvantage vis a vis the larger players, as a result.

We thank you again for the opportunity to share our perspective.

Paul Sieminski	**Holly Hogan**	**Kevin Koehler**
General Counsel	Assoc. General Counsel	Trust & Safety Wrangler