Hearing on "GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation" - March 19, 2019

Gabriel Weinberg
CEO and Founder
DuckDuckGo
Questions for the Record
Submitted April 19, 2019

WRITTEN QUESTIONS FROM SENATOR BOOKER

1. Marginalized communities, and specifically communities of color, face a disproportionate degree of surveillance and privacy abuses. This has been the case since the Lantern Laws in eighteenth-century New York City (requiring African Americans to carry candle lanterns with them if they walked unaccompanied in the city after sunset) up through the stop-and-frisk initiatives of more recent years.

   There are echoes of this tradition today in the digital realm as marginalized communities suffer real harm from digital discrimination. For example, in recent years we have seen many instances of housing discrimination and digital redlining, employment discrimination through digital profiling and targeted advertising, exploitation of low tech literacy through misleading notice and choice practices, discriminatory government surveillance and policing practices, and voter suppression and misinformation targeting African Americans and other minorities.

   I am concerned that—rather than eliminating the bias from our society—data collection, machine learning, and data sharing may actually augment many of the kinds of abuses we fought so hard to eliminate in the Civil Rights Movement. We need privacy legislation that is centered around civil rights.

   a. In your view, is a private right of action critical to protecting the civil rights of individuals affected by data collection and disclosure practices?

   Yes, a private right of action is critical to protect the civil rights of individuals affected by data collection and disclosure practices.

   b. How easy is it for seemingly non-sensitive information like a ZIP Code to become a proxy for protected class or other sensitive information? How can that information be used to discriminate?

   It is extremely easy for seemingly non-sensitive information like a ZIP Code to become a proxy for protected class or other sensitive information. That information then can be readily used to discriminate. For example, even with excluding ZIP Codes, a company can segregate people who follow local businesses in that zip code – and those "likes" have been shown to be correlated to location, age, gender, etc. That data can then be used to discriminate vis-a-vis certain categories of people.

c. Significant amounts of data about us are gathered by companies most people have never heard of. Do we need a registry of data brokers, similar to what Vermont established last year?

A registry of data brokers would be helpful in that it would ideally provide a basis for individuals to readily remove themselves from those databases.

2. The tech journalist Kashmir Hill recently wrote a widely circulated article on her efforts to leave behind the "big five" tech companies—Facebook, Google, Apple, Microsoft, and Amazon. Using a VPN, she blocked all of the IP addresses associated with each company and then chronicled how her life changed. She experimented first by blocking individual companies, and then, at the end of the series, she blocked all five at once. Ms. Hill found that—to varying degrees—she could not get away. Repeatedly, her efforts to intentionally block one company created unpredictable ripple effects for engaging with other, seemingly unrelated, companies and services. Ms. Hill's article spoke to how pervasive these companies are and how much data they capture about us when we're not even (knowingly) using their services.[1]

   a. How would you respond to the following argument? "If people are uncomfortable with the data practices of certain tech companies, they simply shouldn't use their services."

   People should vote with their feet to the extent they can. For example, we offer a compelling private alternative to Google search, and similarly compelling private alternatives exist for most other services. It cannot be denied, however, that some situations make it extremely difficult to avoid the services of certain tech companies. An illustrative example is the Department of Commerce's National Institute of Standards and Technology recent initiative to engage stakeholders in the creation of a privacy standard – the project uses Google Groups. See https://groups.google.com/a/list.nist.gov/forum/#!forum/privacyframework.

   b. What does providing consent mean in a world where it's extremely difficult to avoid certain companies?

   The notice-and-consent model is fundamentally broken and has been for a long time. When consent is not perceived as optional, is not fully understood, or does not work as expected, it is not actually consent.

3. It would take each of us an estimated 76 working days to read all the digital privacy policies we agree to in a single year.[2] Most people do not have that much time. They might prefer something simple, easy, and clear—something much like the Do-Not-Track option that has

[1] Kashmir Hill, I Cut the 'Big Five' Tech Giants from My Life. It Was Hell, GIZMODO (Feb. 7, 2019), https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.

[2] Alexis C. Madrigal, Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days, ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you- encounter-in-a-year-would-take-76-work-days/253851.

been featured in most web browsers for years.

However, there is a consensus that Do-Not-Track has not worked, because despite the involvement and engagement of stakeholders across the industry, only a handful of sites actually respect the request. A 2018 study showed that a quarter of all adult Americans were using Do-Not-Track to protect their own privacy—and yet 77 percent of Americans were unaware that Google, Facebook, and Twitter don't respect Do-Not-Track requests.[3] Just last month, Apple removed the feature from its Safari browser because, ironically, Do-Not-Track was being used for browser fingerprinting, i.e., having the feature turned on was used to distinguish individual users and track them across the web.[4]

a. What purpose does a notice-and-consent regime serve if the most prominent consent mechanism is only regarded as a suggestion at best?

The notice-and-consent model is fundamentally broken and has been for a long time. When consent is not fully understood or does not work as expected, it is not actually consent.

b. How much faith should the failure of Do-Not-Track give us in the ability of the industry stakeholders to regulate themselves?

Self-regulation in the privacy field has not worked. We need a Do-Not-Track law.

c. In your view, should this approach be abandoned, or would federal legislation requiring companies to respect the Do-Not-Track signal breathe new life into the mechanism?

Do-Not-Track is a viable solution, but it needs legal teeth. Federal legislation requiring companies to respect a Do-Not-Track signal would be a massive step forward in privacy protection.

4. Given that California has enacted its own privacy legislation that will take effect next year, much of the discussion at the hearing centered on how a federal data privacy law will affect state-level efforts to regulate in the same space. However, most of our existing privacy statutes do not include provisions to overrule stricter protections under state law.[5] These preemption provisions are the exception rather than the rule, and became more prevalent starting in the 1990s in statutes like the Children's Online Privacy Protection Act of 1998, the CAN-SPAM Act of 2003, and the 1996 and 2003 updates to the Fair Credit Reporting Act.

[3] The "Do Not Track" Setting Doesn't Stop You from Being Tracked, DUCKDUCKGO BLOG (Feb. 5, 2018), https://spreadprivacy.com/do-not-track.

[4] Ahiza Garcia, What Apple Killing Its Do Not Track Feature Means for Online Privacy, CNN (Feb. 13, 2019), https://www.cnn.com/2019/02/13/tech/apple-do-not-track-feature/index.html.

[5] The following statutes do not preempt stricter protections under state law: the Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Drivers' License Privacy Protection Act, and the Telemarketing Consumer Protection and Fraud Prevention Act.

a. In your view, should a federal data privacy law preempt state data privacy laws? Why?

It is premature to discuss preemption until a stronger-than-state-law federal privacy bill is close to enactment. And even then, any preemption should be narrowly constructed so that states can adequately respond to the rapidly unfolding privacy landscape.

b. In your view, should a federal data privacy law implement the requirements of the California Consumer Privacy Act as a floor? If not, please explain the most significant change you would suggest.

We support robust amendments to the California Consumer Privacy Act. See https://spreadprivacy.com/ccpa-privacy-for-all-act/. Because CCPA is not as strong as we believe it should be, we support a CCPA-plus-more as a floor for a federal data privacy law.

c. The specific wording of a proposed preemption provision will invite considerable debate in Congress and, ultimately, will still require courts to interpret and clarify the provision's scope. Should the Federal Trade Commission have notice-and-comment rulemaking authority to aid in the statute's interpretation and to clarify which types of state laws are preempted? Or, alternatively, is case-by-case adjudication of multiple state privacy laws preferable? Would rulemaking authority obviate the need for Congress to solve each and every preemption issue in drafting the text?

It is premature to discuss preemption until a stronger-than-state-law federal privacy bill is close to enactment. As such, we express no opinion at this time on how preemption should be operationalized.

d. The preemption language in, for example, the amendments to the Fair Credit Reporting Act was included as part of a heavily negotiated process in which consumers received a package of new rights in exchange for certain preemption provisions.[6] Rather than centering the federal privacy bill debate on the existence of a preemption provision, shouldn't our starting point be: "Preemption in exchange for what?" In other words, what basic consumer protections should industry stakeholders be willing to provide in exchange for preemption? Do the requirements of the California Consumer Privacy Act represent a good floor for negotiating preemption?

We support robust amendments to the California Consumer Privacy Act. See https://spreadprivacy.com/ccpa-privacy-for-all-act/. Because CCPA is not as strong as we believe it should be, we support a CCPA-plus-more as a floor for a federal data privacy law.

5. At the hearing, several witnesses indicated that opt-out requirements that permit users to tell

[6] The 1996 and 2003 amendments included, for example: new obligations on businesses to ensure the accuracy of reports, increased civil and criminal penalties, remedial rights for identity theft victims, and the right to free annual credit reports.

companies not to process and sell their data are more protective of data privacy and more conducive to the user experience, since they do not impose the "take it or leave it" dynamic that opt-ins tend to create. In your view, are opt-outs preferable to opt-ins in terms of both data privacy and user experience? Why?

Discussion of opt-out and opt-in is confusing because those terms' meaning turns on what the default setting is. For example, if a user "opts-in" to having do-not-track signals turned on for all websites, and then a website abides by that signal, is that "opt-out" or "opt-in?" We support any system that recognizes privacy as a fundamental human right and allows individuals to easily and effectively exercise that right.

6. At the hearing, several witnesses also indicated that the Federal Trade Commission, and perhaps state attorneys general, should have primary enforcement authority for data privacy violations. In your view, what additional authority and/or resources would the FTC need to perform this function effectively?

Because privacy is a fundamental human right, we believe in a private right of action that allows people to legally defend their right to privacy. With regard to the FTC in particular, we do not believe the agency has adequately protected consumer privacy. Therefore, we are unpersuaded that additional statutory authority or financial resources would necessarily change the FTC's direction in this regard. Instead, consumers would be better served by stronger state and federal laws, such as a Do-Not-Track law.

****

WRITTEN QUESTIONS FROM SENATOR DICK DURBIN

1. Your company has recognized the strong consumer desire for online privacy.

    a. In general, do you support the idea of creating a "right to be forgotten" for childhood online activity?

    We have not yet had occasion to consider this policy question, and therefore take no position on it.

    b. Specifically, do you support giving individual Americans an enforceable right to request that commercial websites and online services delete personal information that was collected from or about the individuals when they were children under age 13?

    We have not yet had occasion to consider this policy question, and therefore take no position on it.

2. It seems like so much of today's intrusive data collection is really about targeted internet advertising. Your company is refreshing in that it does not use microtargeted, behavioral advertising. Instead, you protect your users' privacy and only use ads that are related to a user's current search, not the user's search history or other personal data.

How much do you think it would help Congress' efforts to reduce intrusive data collection if we gave American consumers the ability to exercise a blanket opt-out for online targeted advertising?

It would be immensely helpful in reducing intrusive data collection if Congress were to pass a law that gives American consumers the ability to exercise a blanket opt-out for online targeted advertising. A well-drafted Do-Not-Track law would do exactly that.

****

WRITTEN QUESTIONS FROM SENATOR LINDSEY O. GRAHAM

1. What was your estimated initial cost (both time and expense) to become GDPR compliant?

Because DuckDuckGo has always respected user privacy and has long had a business model that does not collect or share user data, we did not need to undertake significant efforts to become GDPR-compliant. We did not have in-house counsel prior to GDPR's effective date, so we did hire outside counsel (at a highly respected, international law firm) to consult with us on the subject, to ensure we understood the contours of the law. Our outside counsel fees were approximately $10,000. We had one employee who led the interactions with outside counsel and met with each of our company's functional teams to review their data collection, use, and retention practices (or lack thereof).

2. What are your estimated recurring annual GDPR compliance costs (both time and expense)?

De minimus.

3. What is your estimated initial costs (both time and expense) to become CCPA compliant?

Because DuckDuckGo has always respected user privacy and has long had a business model that does not collect or share user data, we do not need to undertake significant efforts to become CCPA-compliant. In fact, we are already compliant, which we know as a result of GDPR-compliancy efforts in 2018, namely a thorough review with each of our company's functional teams to review their data collection, use, and retention practices (or lack thereof).

4. What are your estimated recurring annual CCPA compliance costs (both time and expense)?

De minimus.

5. Are you differentiating your products based on consumers or businesses in the EU and California?

We do not differentiate our products in terms of privacy rights or features. Consumers in different regions of the world can customize our products to their local region, such as selecting a localized language.

6. What are the specific areas of the CCPA that could have a negative impact on competition and innovation? What areas of the CCPA need more clarity, improvement, or removal?

We support robust amendments to the California Consumer Privacy Act. See https://spreadprivacy.com/ccpa-privacy-for-all-act/.

****

WRITTEN QUESTIONS FROM SENATOR CHUCK GRASSLEY

1. Please briefly explain the importance of transparency and ensuring that consumers can make informed decisions about the information they share.

While we believe transparency is critical to ensuring that consumers can make informed decisions, we believe it is even more important to recognize that the notice-and-consent model is fundamentally broken and provide more effective mechanisms for consumers to take control of their privacy.

2. Transparency is critical in ensuring that consumers can make informed decisions. That can become more complicated, however, as our lives are increasingly connected to the technologies around us, like autonomous vehicles. According to one report, by 2025 each person will have at least one data interaction every 18 seconds – or nearly 5,000 times per day.[7]

   a. How do we balance the need for transparency and informed consent with the reality of our increasingly data-connected daily lives?

In short, it is not practically possible for an individual to meaningfully participate in a notice-and-consent model in the reality of the modern world. A solution is a federal law, like a Do-Not-Track law that only requires a person to turn on a "do not track" setting (once and be done), with the law then requiring companies to obey that signal.

   b. Should consumers have to consent to every data interaction throughout their day?

No. The notice-and-consent model is fundamentally broken and practically useless in the modern world.

3. If Congress enacts federal data privacy legislation, how do we ensure that companies are still incentivized to innovate in their privacy and data protections, rather than just 'check the box' of regulatory compliance?

A private right of action would help to ensure companies cannot use federal data privacy legislation as a shield against enforcement.

[7] David Reinsel et al., *The Digitization of the World—From Edge to Core*, IDC (Nov. 2018).

****

WRITTEN QUESTIONS FROM SENATOR KAMALA HARRIS

Private Right of Action in the Event of a Data Breach

In your testimony, you wrote that "privacy legislation, like the GDPR and CCPA, is not only pro-consumer, but also pro-business." Among the protections afforded consumers by the CCPA is a limited private right of action, which helps to ensure compliance with the law by allowing consumers to seek civil remedies in certain circumstances where their personal information is compromised by a data breach. Stakeholders and government officials in California are considering expanding the CCPA's private right of action to cover the unauthorized sharing, sale, and use of consumers' data.

1. Does DuckDuckGo support the right of consumers to seek justice in a court of law when their private information is misused by a company or compromised in a data breach?

Yes, we support the right of consumers to seek justice in a court of law when their private information is misused by a company or compromised in a data breach.

2. How does the CCPA's current private right of action affect DuckDuckGo's business practices?

Because the CCPA's current private right of action is so narrow, and because our business does not collect or share user information, our business practices are not materially impacted by the CCPA's current private right of action.

3. Does DuckDuckGo support building upon the consumer protections in the CCPA by expanding the private right of action to cover other violations of the Act?

We support robust amendments to the California Consumer Privacy Act, including an expansion of the private right of action to cover other violations of the Act. See https://spreadprivacy.com/ccpa-privacy-for-all-act/.

Preemption

During the hearing, several of the witnesses testified in favor of a federal data protection law that builds upon the privacy standards in the CCPA, but that preempts state law and would effectively bar states from enforcing their own data protection measures.

4. As an entrepreneur who has made privacy and data protection central to your business's identity, do you have concerns about Congress setting a federal standard that would foreclose the ability of states to innovate by enacting and enforcing data protection measures in the future?

Yes, we are concerned that Congress might set a federal privacy standard that would foreclose the ability of states to innovate by enacting and enforcing data protection measures in the future. We believe it is premature to consider preemption at this time.

****

WRITTEN QUESTIONS FROM SENATOR MAZIE K. HIRONO

1. During the hearing, I mentioned that there is significant evidence that a consumer's privacy settings are "sticky," with consumer's rarely altering their default privacy settings.

Do you agree that the vast majority of consumers rarely change their default privacy settings?

Most consumers rarely change their default privacy settings – but a large number of them do. For example, we find that about a quarter of consumers have enabled their "Do Not Track" browser setting. See https://spreadprivacy.com/do-not-track/.

2. In view of the "sticky" nature of privacy settings, my inclination is to have a system in which, by default, a consumer is considered to have opted out of data collection and a company can only collect that consumer's data if the consumer expressly opts in to data collection.

   a. Do you think an "opt-in" privacy regime is the right approach?

   Discussion of opt-out and opt-in is confusing because those terms' meaning turns on what the default setting is. For example, if a user "opts-in" to having do-not-track signals turned on for all websites, and then a website abides by that signal, is that "opt-out" or "opt-in?"

   In any case, we agree with what you describe here. We believe that Do-Not-Track legislation is the right approach, in which companies are required to abide by a user's do-not-track signal, which would be set once and then apply everywhere.

   b. How would you ensure that each consumer is aware that his or her data is being collected and that the consumer consents to that collection?

We do not believe it is possible merely through "notice" or consumer education to ensure that consumers are aware of the depth and breadth of how companies collect, use, and share consumer data; and without that baseline knowledge, consumers cannot effectively consent.

3. We often hear that federal privacy legislation shouldn't be too tough or it will kill small businesses and stop innovation.

How does your company both protect the privacy of its users and manage to turn a profit?

Rigorous federal privacy legislation will not kill small business or stop innovation. In fact, we believe rigorous federal privacy legislation will help small businesses thrive and increase innovation. We, for example, both protect the privacy of our users and are a profitable business due to our creation of innovative products. See https://spreadprivacy.com/duckduckgo-revenue-model/.

****

WRITTEN QUESTIONS FROM SENATOR AMY KLOBUCHAR

DuckDuckGo has expressed support for the European Commission's investigations and fines against Google for anticompetitive behavior under European law. You have also publicly detailed specific competition-related complaints about Google's business practices.

- Within the last year, has the FTC or Department of Justice contacted you or others at DuckDuckGo in connection with an investigation into Google's business practices, or do you have any reason to believe that such an investigation is underway?

No, no one from the FTC or the Department of Justice contacted me (or anyone at DuckDuckGo) in the last year, or even the last several years, in connection with an investigation into Google's business practices. We have no reason to believe that any such investigation is underway – other than the common-sense belief that such an investigation <u>ought</u> to be happening, given Google's almost complete domination of the online search market. See https://sparktoro.com/blog/2018-search-market-share-myths-vs-realities-of-google-bing-amazon-facebook-duckduckgo-more/.