July 12, 2019

The Honorable Anna Eshoo
U.S. House of Representatives
202 Cannon House Office Building
Washington, DC 20515

The Honorable Zoe Lofgren
U.S. House of Representatives
1401 Longworth House Office Building
Washington, DC 20515

RE: Main Street Privacy Coalition Comments on
Draft Framework of the Online Privacy Act of 2019

Dear Representatives Eshoo and Lofgren:

We appreciate your willingness to seek comment on the Draft Framework of the Online Privacy Act ("Draft Framework"). The undersigned associations of the Main Street Privacy Coalition ("MSPC") represent over a million Main Street businesses in industries that directly serve their consumers, help support communities across the country, and that Americans know and interact with every day. Collectively, the industries that MSPC trade groups represent directly employ nearly 34 million Americans and constitute over one-fifth of the U.S. economy by contributing approximately $4.5 trillion (or 21.8%) to the U.S. gross domestic product (GDP).

Our member companies have no higher priority than maintaining a positive relationship with their customers. One key aspect of those relationships is respecting the personal information that customers share with businesses. Virtually every industry sector – whether consumer-facing or business-to-business – handles significant volumes of consumer information so they can provide the level of service their customers expect. To comprehensively protect Americans and earn the confidence of consumers, any federal data privacy framework should apply to all industry sectors, and not contain any loopholes, carve-outs or alternative regulatory schemes that leave consumers unclear about how their data is protected or, even worse, totally unprotected under the law. Every entity involved in handling data should have an equivalent obligation under the law to properly guard the data, and legislation should not rely solely on private contracts to create those legal obligations for certain sectors.

With these precepts in mind, there are a few areas of the Draft Framework that, as set out below, merit further consideration and revision in future versions of the framework.

<u>Industry Neutrality: Reconsider Service Provider Exemption</u>

Under the Draft Framework, "service providers" are exempt from the requirements of Title I, which ensures user privacy rights. In fact, it is not simply that service providers would have special rules or allowances when it comes to user rights – service providers would not be covered by Title I of the bill *at all*. That type of construct would actually impair consumer privacy rights. As broadly defined, "service providers" would include telecommunications companies, Internet Service Providers, large data storage companies, as well as data and payment processors and networks, many of which are nationwide corporations with vast resources. While these companies may not "control the selection or transformation" of data, and thereby qualify for the service provider exemption, they handle large volumes of personal information and often

profit from its use. Service providers also routinely use personal information to tailor services to consumers – including personalized advertising. All of this data processing would be permitted under the Draft Framework in a regulatory-free zone, and consumers would not have the right to access, correct, delete, or port the personal information used by these entities. Consumers also would not have the right to be informed about the collection of their personal information, or to opt-out of personalized content, as is required of other entities under the Draft Framework.

The service provider exemption may even allow businesses to sell personal information without permission. If service providers allow other businesses to "select" which information those businesses want to purchase, they might still fit within the service provider definition and yet maintain their broad exemption from Title I.

Data privacy legislation should not include a service provider exemption for entities that handle consumer data. If service providers, or any other businesses, do not use or maintain any personal information, then the requirements of Title I of the Draft Framework would not create obligations for them in the first place, so an exemption from that title is unnecessary. Where entities in any industry maintain or handle consumer data, privacy legislation should place direct statutory obligations on them based on how they collect, process, disclose and otherwise use personal information. Creating a carve-out up front, however, as the Draft Framework does for service providers, creates risks that businesses will find more and more creative ways to use consumer data while the law shrouds the existence and details of that data use from consumers; directly contradicting and undermining the spirit and purpose of the law.

Reconsider Intent Requirement

The Draft Framework's exemption for "unintentional collection/processing" also merits closer examination. Requiring that businesses have "actual knowledge" of "specific" personal information they have collected in order to be subject to Title I of the bill creates a high bar. It is not clear how the phrase "actual knowledge" would be defined or interpreted by courts, or how it would be imputed to a business. Given the substantial use of artificial intelligence and similar algorithms involved in the processing and use of personal information, standards involving intent and knowledge may open unintended loopholes in privacy legislation.

For example, consideration should be given to protecting against interpretations of this language that suggest there is an exemption for entities that do not directly collect data from a consumer. If entities that do not "collect" personal information directly from consumers are not covered by the privacy framework, then a vast ecosystem of business-to-business data collectors (e.g., Cambridge Analytica), data brokers and other processors or storers of data collected by consumer-facing entities could avoid the regulatory requirements imposed on other businesses. If a consumer were to exercise a privacy right to delete data, but the data storage vendor (which did not directly collect the data from the consumer) is exempt from the obligations of the law, the consumer may never be able to fully exercise his or her deletion right as the law would not reach the vendor. This is inconsistent with the expectations of the consumer, and exemptions for entities that do not directly collect personal information from consumers should be eliminated.

Remove Data Breach Notification Exemption

Title II, section 10 of the Draft Framework lays out data breach notification requirements. However, the Draft Framework only applies to businesses that have a direct relationship with the individual whose data was breached. This would exempt many large data-aggregating and data-brokering businesses that energetically participate in a secondary market for consumer information. These businesses, should be responsible for notifying people about their own breaches as a matter of fairness and expediency. The breached entity, after all, is in the best position to investigate the breach, ascertain the risk of harm, and be accountable to affected individuals for a data breach. Yet, the Draft Framework would exempt certain breached entities from its requirements. The vast majority of Main Street businesses that have direct consumer relationships are small businesses that should not be on the hook for the costs and potential liabilities relating to breaches suffered by well-resourced businesses in the secondary market.

Some will argue that businesses without a direct consumer relationship do not have the necessary contact information to provide breach notifications. This is a red herring, as history shows that breached service providers in a number of instances have notified the affected individuals of their consumer-facing clients following the service provider's breach.[1] Having the direct consumer relationship also does not necessarily increase the chances that a business has contact information for the affected individuals. For example, many corner stores and restaurants that consumers interact with every day do not collect contact information on their millions of customers. A name and payment card number may pass through their systems, but typically nothing more does. On the other hand, credit reporting agencies and many other businesses that are most active in the secondary market for consumer information have a great deal of personal information about consumers, including contact information. Whether a business does or does not have contact information, then, should not be determinative of whether that business has the legal responsibility to ensure it provides notice of data breaches. Rather, it is the entity that suffers the breach that should be primarily accountable to affected individuals.

Solving this issue is not challenging. Many state data breach laws have adopted alternative, public notice options (often called "substitute notice" provisions) for businesses to notify affected consumers when they have data breaches but do not have contact information for affected individuals. There is no reason why breached service providers could not do the same when they are aware they have suffered a breach of sensitive information that presents a risk of harm to affected individuals. This substitute notice option is probably necessary for any breach law to work, and it makes far more sense than allowing some businesses to foist their breach notification responsibilities onto other businesses that had nothing to do with the breach itself.

Preserve Incentives for De-identifying Data

Title I, section 8 of the Draft Framework properly includes an exemption for data that has been de-identified. There are many ways to de-identify data including a variety of encryption and tokenization technologies. But, the exemption states that it does not apply to data that can be

[1] https://www.t-mobile.com/customers/experian-data-breach

reidentified "using other data stored by the covered entity." This language removes important incentives to encrypt or otherwise obscure data. Businesses need to have a way to de-encrypt or de-tokenize their data. The tools to do that may be stored by the business itself – sometimes behind additional firewalls or on a separate part of their data systems. Some businesses may rely on other companies to store that data. Regardless, broadly saying that any business that stores de-encryption keys (even if segregated according to industry best practices) will make it less likely that businesses will use encryption or tokenization technologies in the first place. That would be an unfortunate outcome for a provision that appears to be intended to create incentives for the use of these technologies.

Protect Against Antitrust Abuses

The Draft Framework includes giving consumers a "right of portability" of their data in Title I, section 4. There are important concerns about data portability rights and their potential for creating competition law and policy problems. There are many pieces of consumer information – such as transaction records – that are inextricably tied to sensitive or confidential business records. Such sensitive business records should not be portable. If they are, then companies can and will create incentives for their customers to request data from competitors and then provide the data to those companies. If some companies are able to gain sales records from their competitors and aggregate them, the "right of portability" will be transformed into an instrument of industry consolidation and monopolization. That outcome should be carefully avoided. Additionally, data ported in the aggregate could lead to violations of intellectual property rights engineered from that data; portability itself could disincentivize future innovation. Finally, the security of consumer data would be jeopardized if companies are incentivized to increase the flow of data from one company to another.

Modify Information Security Requirements

The Draft Framework sets out information security requirements in Title II, section 9. We agree with the overriding principle of the requirements in the Draft which call for the agency established by the Draft to promulgate regulations requiring "reasonable information security policies and procedures." We think that is the right policy and a good way to get to strong information security. But, section 9b of the Draft Framework then ties the new agency's hands and creates inappropriate requirements for some businesses by instructing the agency on specifics of those regulations. Those specific requirements – including identifying an information security officer, and setting a number of processes regarding foreseeable vulnerabilities and disposing of information – are both woefully insufficient for some businesses and strikingly over-regulatory for others, depending on the size and scope of the business. For large, sophisticated businesses that handle very sensitive consumer data, none of the specifics listed in 9b will be remarkable. In fact, they will be elementary-level security basics that such businesses should be engaging in already. But, for millions of small businesses that our associations represent, these specifics are unhelpful and inappropriate. Take, for example, a corner restaurant or convenience store at which the store owner works in the store serving customers 50-60 hours per week – a regular occurrence. To require that person to identify an

information security officer, detail foreseeable risks, and a develop a formal process to mitigate those risks simply does not make sense. These small businesses serve many individuals and have data (especially payment data) that pass through their systems, but they rely on much larger businesses to do the jobs of transmitting, processing and protecting such data. These small businesses should not be saddled with unnecessary paperwork requirements that create unreasonable burdens on them, which could negatively impact the success and growth of small businesses, and deter future entrepreneurs from entering the market.

The bottom line for information security is that the agency should have discretion to tailor its regulations based on the factors outlined in the Draft Framework – and without prejudging that outcome with specific requirements that tie the agency's hands and do not materially advance the state of information security.

Avoid a Litigation Mess

The Draft Framework creates a private right of action in Title IV. In our view, enforcement by federal agencies and state attorneys general should be adequate to ensure widespread compliance with this type of law. In many areas, plaintiffs' lawyers have created litigation factories to send demand letters and file countless lawsuits for minor violations of laws that include private rights of action. From patents to disability cases and more, these thousands of demand letters and cases brought by litigation "trolls" cost businesses millions and clog the courts, but provide almost no benefit to consumers. In fact, many of these threatened or filed suits include claims on behalf of "customers" that have never seen or visited the businesses in question. Plaintiffs' lawyers are simply pulling broad lists of businesses to develop target lists to which they can send millions of demand letters with legal claims. Even if the majority of those claims have no merit whatsoever, the lawyers are rewarded with some form of payment because the cost to the targeted business of hiring counsel to fight the baseless claims and have them dismissed often costs much more than the payouts being sought for the case to be withdrawn. Privacy legislation should not act to turn on a new spigot of meritless claims, which is simply bad policy, unjustifiable, and serves to reduce the resources that could be spent developing more robust and privacy-protective systems.

There are already plentiful legal mechanisms that exist to protect consumers if they are injured by businesses' behavior – including in the handling of data. There is no need for a federal privacy law to create a new cause of action that paves the way for an explosion of meritless claims. In short, Congress should not create a new cottage industry for privacy trolls.

Questions

We appreciate your willingness to produce the Draft Framework and provide us with an opportunity to comment on it at this early stage. We recognize that this means some aspects of the Draft Framework that would be further detailed in legislative language might not yet be decided or explained. With that in mind, there are a few key areas of the proposal at this stage that raise questions we see as important to the development of a piece of legislation and on

which we would be interested in engaging with you as you move toward draft legislation. These question areas include the following:

- The definition of "personal information" needs to be carefully considered and should be more precisely tailored to avoid the unintended consequences of an overly broad definition that sets the scope of the entire bill's application. The Draft Framework defines personal information as "any information that is linked or reasonably *linkable* to a specific individual." In the digital age, it is hard to imagine any data that is not "linkable" to an individual. The fact that a retail customer may have a shoe size of 6, however, is hardly the kind of sensitive data that presents a risk of a privacy harm, even if that fact is the subject of a data breach. This is why Nevada recently enacted an online privacy law with a more narrowly tailored definition of personal information that specifically defines the categories of personal information that would pose a significant risk to the consumer in the event of a data breach.[2] Businesses have finite resources, and should use their limited resources to protect the most sensitive information that creates risks of harm to individuals. We urge you to consider the broad definition in the Draft Framework and appropriate ways to narrow its application so that resources can be properly allocated to protecting the kind of data that consumers expect to be protected and for which they wish to exercise privacy rights, as opposed to any type of data possible.
- Title II, section 3 of the Draft Framework includes limitations on selling data. How a sale of data is defined is a key question for any privacy legislation. Some states have defined a data sale much too broadly such that it covers the sharing of data that small businesses must engage in to handle their data in a similar manner to larger businesses. "Selling" should be more narrowly defined to the concept that most people think of as a traditional sale. For example, the definition of a sale could be limited to the exchange of personal information for monetary consideration by the covered entity to a third party. Such a definition, which was recently adopted in the Nevada online privacy law, would ensure that a sale is not defined in way that leads to an overly broad regulatory scope with unintended consequences for data that is routinely "shared" for legitimate business purposes. It is instructive to review the General Data Protection Regulation (GDPR) adopted by the European Union with respect to the six legal bases for data-processing which includes sharing information for these purposes. Lastly, the fact that contractors must be hired to engage in some business operations functions that require the sharing of customer data should not be inadvertently implicated by how a data sale is defined.
- Title I, section 5 creates a right of human review. There are many concepts that are not fully defined in the current description of this right including what it means for a decision to be made by an "automated process," what it means to create or increase a privacy harm, and what counts as a "significant" privacy harm. All of these concepts will be important in determining the proper scope of any right of human review. Furthermore, there are many instances, such as automated reviews of job applicants' resumes to scan for credentials required for a particular job (e.g., holds a particular professional

[2] *See* Nev. Rev. Stat. §§603A.040(1) and (2).

certification), that should not be subject to a right of human review as such a requirement in these instances could significantly slow the ability of companies to hire qualified employees. Additionally, with respect to processing user requests related to privacy rights, a human review right could be self-defeating if businesses cannot use automated processes to triage and address consumer privacy requests in a timely manner. The inability to use automated processes to timely fulfill consumer privacy requests may not only place greater burdens on consumers, but also greater costs on businesses and subject them to the risk of government enforcement proceedings or litigation. For these reasons, if a human review right is included in the framework, it should be limited to specific instances in which such a review is necessary and would not overburden consumers or businesses.

- Title I, section 6(b) of the Draft Framework requires that covered entities "must provide a non-personalized version of the service" to consumers. It is unclear whether businesses that rely on personalization services would be capable of providing a non-personalized version if it is fundamental to the service they offer. In these instances, such a requirement could amount to a mandate to create an unnecessary business operation that has no viable purpose. We imagine that this would not be the intent of such a provision, but absent further requirements or explanation, it is unclear how such a requirement would be limited and how businesses might comply with it. If the intent is to address the issue of cookies, then a narrower approach that may enable broader compliance would be to require disclosure of a website's use of cookies and allow users relevant choices. We look forward to learning more about the intent of this provision and determining if the public policy interest may be achieved in a more targeted manner that would not raise the concerns noted above.
- Title I, section 8(d)(i) states that a business may deny a request if the individual's identity cannot be confirmed. This is especially important, because one user could pose as another user in order to gain access to the other person's information. The framework could address this by requiring specific documents regarding an individual's identity be given to the business before it is required to comply with a request. We would suggest inclusion of clear standards as to what constitutes a valid request to trigger a business's obligation to respond to a user request, including the documents to be provided, the number of requests allowed for each user per year, and the time period permitted to respond to such requests.
- Title II lays out provisions relating to notice and consent requirements. One aspect of this that is essential for many Main Street businesses is the concept of "implied consent" that is captured in the Draft. The industries we represent have extensive experience and insight into a variety of customer interactions that properly fall within the concept of "implied consent" and we would very much like to work with you to ensure that those concepts are properly captured in your work moving forward.
- Title II, section 6 includes provisions on data minimization. There are many questions that come up when working through data minimization concepts including competing claims for data preservation due to law enforcement and other concerns. Many questions remain to be answered regarding how extensive a data minimization regime could be

consistent with other business responsibilities. The requirement of data "substitution" in particular raises many questions. Creating a requirement in this area could impose a large cost burden and raise antitrust issues if particular technologies are mandated. The way this is done and how broadly it applies are important to the workability of data substitution.

* * *

Thank you again for the opportunity to comment on the Draft Framework. We hope that these comments are helpful to your work and look forward to discussing them with you as you work through the legislative drafting process.

Sincerely,

The American Pizza Community

International Franchise Association

National Association of Convenience Stores

National Association of Home Builders

National Association of Realtors

National Association of Truck Stop Operators

National Council of Chain Restaurants

National Grocers Association

National Restaurant Association

National Retail Federation

Petroleum Marketers Association of America

Society of Independent Gasoline Marketers of America