STARRY 38 Chauncy Street, 2nd Floor
Boston, MA 02111

May 29, 2019

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580

Re: Hearings on Competition and Consumer Protection in the 21st Century; Hearing 12: the FTC's Approach to Consumer Privacy

Chairman Simons and Commissioners:

Starry, Inc. (Starry) is encouraged that the Federal Trade Commission (FTC) is undertaking a fresh review of its approach to consumer privacy. Consumer privacy is under attack in the physical and digital realms, and the government must act quickly to upgrade and modernize its policy and enforcement frameworks to adequately protect consumer privacy. The time to act is now and the FTC is uniquely positioned to take a global leading role in privacy protection.

In order to effectively engage consumers, Starry respectfully suggests that the FTC create a ***Privacy Compact with Americans***, a set of baseline commitments on which the agency outlines its basic tenets of consumer privacy protection. This *Privacy Compact* would serve as guiding principles for the FTC and also enable the agency to iterate more detailed policies, protections, and enforcement actions over time. It is a simplistic starting point, but it's a significant improvement over the lack of any formal federal commitments.

The *Privacy Compact* would form the basis for future privacy actions without having to establish an all-encompassing framework from the ground up. Laying down a marker and creating an easy-to-understand set of privacy commitments would be a tremendous benefit to consumers, who today struggle to understand their privacy rights and the government's role in protecting them. Developing this *Privacy Compact* would be transformative to the privacy debate and create a global model.

We provide additional details and context below, and first explain how Starry, as an ISP, protects our customers' privacy.

Starry's Approach to Privacy

At Starry, our perspective on consumer privacy is simple: 1) the information we collect is the customer's information, not ours; and 2) it's our obligation to be a good steward of that information. When we collect information from our customers – or potential customers – we treat that information as theirs and use it for extremely limited purposes aimed at serving them. We strive to be as transparent as possible,

so we also consider whether a customer can easily understand - or if they would be surprised to know - how we are using a piece of information they have provided to us. If it is not clear, we continuously iterate on our policy to ensure that we adequately and clearly explain what information we are collecting and for what purpose.

We take this approach because we built a customer-centric business that does not rely on the collection, aggregation, and use of customer information, except in the most basic ways necessary to sign someone up for service and to market our service to them.

We are an ISP, and we recognize that we hold a special place in people's lives – we are the bridge to their digital life and we take that role incredibly seriously. Most importantly, we do not exploit this relationship to create other businesses or revenue streams. We generate revenue by connecting our users to the internet, and that's it. We are not a content company, a big data company, an advertising company, or a content platform. We carry this mindset through our work and our corporate culture: customer-first means providing great service, and it means protecting our customers' privacy.

Our approach to privacy can be distilled into a few key commitments, which we proudly make to all of our customers:

- When you subscribe to and use our service, we collect information for limited purposes including providing internet service, improving your internet service experience, and marketing our service and other Starry products and services to you.

- We do not sell any of the information we collect through our service, even if it is de-identified, aggregated, or otherwise obfuscated.

- We only share information about you with third parties in the limited circumstances described in our Privacy Notice, including to provide or improve our products and services, when it is required by law, or when we have your explicit consent.

- Your web browsing history is your business, not ours. We will not use or share information about the websites you visit when you are using our internet service for marketing or advertising purposes.

We also constantly strive to improve our policy and enhance transparency with our customers and will be rolling out an update to our Privacy Notice this summer to better explain how we use the data that we do collect and to meet the practices outlined in the California Consumer Privacy Act of 2018.

The Opportunity for the FTC to Make Simple, Strong Commitments

From a consumer's perspective, there is a fundamental truth about privacy – if you understand how the company that is collecting your information generates revenue, you understand what they will truly do with your data and the level of trust that you can place in them. Their actions and their need to generate shareholder value far outweigh public platitudes about privacy principles and frameworks. As the saying goes: actions speak louder than words.

In this current environment – with respect to very large platform companies, ISPs, and other large tech companies – the conventional (if somewhat cynical) wisdom is that the cost of a federal privacy regulation that is created through a process that they can influence is a far superior outcome to an antitrust process that they have much less control over. And so, these companies frequently express their willingness to cooperate on enacting strong consumer privacy protections.

We suggest that the FTC (or other agency as the Administration or Congress selects) take these companies at their word and push aggressively to enact strong consumer privacy standards and enforcement. The FTC should exert its power to the greatest extent possible and leverage this unique point in time where the current is flowing with it.

We appreciate that the FTC is taking a diligent approach to understanding the state of the art in privacy and to consider enhancing its existing case-by-case approach to privacy enforcement (to the extent it can). But time is of the essence, and the curve to a comprehensive privacy framework is steep. The FTC should act immediately to put a strong and persistent marker down now, from which it can continue shape and build a larger privacy regime.

The *Privacy Compact with Americans* is a core set of promises protecting all Americans' private information. The Compact would serve as an evergreen set of commitments on privacy that the FTC will protect through its future privacy actions. The FTC has the authority to put this *Privacy Compact* in place as a policy today. And while Congress should act to enhance the FTC's (or other agency's) authority, we believe the FTC has the authority to adopt the *Privacy Compact* as a policy statement now, without waiting for Congressional action.

We acknowledge that the *Privacy Compact* is simplistic and consumer-oriented. It is not the end game – it is a starting point from which the FTC can make a strong statement now to consumers in terms they understand, and from which the FTC (given authority) can build a more comprehensive policy framework that reflects the realities of modern technology, business models, and consumer preferences.

The Privacy Compact with Americans

We suggest that the FTC make this *Privacy Compact with Americans* with respect to their personal information:

All Personal Information is Protected Equally: All information that relates to a person's physical or digital life is personal information and should be treated the same.

Disclosure is Mandatory: Any entity that collects or uses Personal Information must explicitly and clearly explain the Personal Information it is collecting, what it will do with the information, whether they intend to sell it, and the other entities with which it intends to share the information.

Permission is Required: Personal Information can only be collected when the person agrees to have their information collected, and can only be used for the reasons that the person permits. Permission must be renewed at least annually.

Personal Information Collection Must be Minimized: Entities that collect Personal Information must collect the smallest data set necessary to achieve the purpose for which the person provided the information.

Transparency, Transferability, and Deletion are Rights: People have a right to know their Personal Information that an entity currently has, the right to receive that information in a format that is shareable and useable by another party, and the right to quickly delete that information from any entity that holds it.

Combined, these tenets provide a clear set of commitments to all Americans under which the privacy of their Personal Information is prioritized and protected. They also form the baseline from which the FTC can view and approach privacy on a going forward basis. Below we provide additional context for each clause.

All Personal Information is Protected Equally

There are not gradients of Personal Information of varying sensitivity – every single piece of information that relates to a person in a physical or digital way is personal and should be treated the same. A single piece of Personal Information is information that tells the holder something unique about a person, and any single piece of this information can be used to violate a person's privacy in digital or physical environments. And combinations of Personal Information can paint a full picture of a person's physical or digital life. Therefore, every single piece of Personal Information must be protected equally. By defining Personal Information broadly

and simply, the specific elements of information that fit within it can evolve over time.

An expansive view of what constitutes Personal Information will both train firms to collect as little Personal Information as possible and require them to protect any Personal Information in the exact same way – and in the most protective way possible.

Disclosure is Mandatory

Before any entity collects or uses any Personal Information, it must first tell the person in as specific terms as possible what information it will collect, what it will do with the information, whether or not it will sell it (individually or aggregated with other data, even if deidentified), and the third parties with which it will share the information.

A person should be able to fully and simply understand what Personal Information they are providing, why, how the collecting entity benefits, what they as an individual get out of it, and the degree to which that information will propagate away from the collecting party. Then, a person can make informed decisions about the benefit that they derive from sharing the information and whether it outweighs their perceived risk, or the value (or revenue) that that the third party derives from the information.

Permission is Required

Before any entity collects or uses any piece of Personal Information, it must first – and always – ask for the person's permission. With full disclosure of the purpose for which the information is collected and how it will be used, the person can make an informed decision about whether or not it will permit the collector to collect or use the information. Personal information is owned by the person, not by the company collecting it, and the person should retain ultimate control over it.

People should be able to grant this permission in part – for various pieces of information and various uses. Entities collecting the information must seek the consent immediately after presenting a clear disclosure of what information it is collecting and how it will use the information. Consent must be explicit and not implied for every new collection and use, consent should be renewed at least annually.

Personal Information Collection Must be Minimized

The best way to protect people's personal privacy is to not collect or use the information in the first place. Firms should collect the most limited set of Personal Information as necessary to provide the product or service that the person providing the information seeks. And the information that firms do collect should be directly related to the purpose for which it is collected, which in turn should be directly related to the product or service that is offered to the person. In the event that a firm collects information for a purpose other than providing the specific product or service to which the information relates – that is, it is provided in exchange for some

other good or service – this fact needs to be made clear to the person providing the information.

This is increasingly important as many firms are attempting to train Artificial Intelligence algorithms, which require huge amounts of unique pieces of data. These firms are most likely to over-collect information and use the information outside of the context of the purpose of the relationship with the user.

Transparency and Transferability are a Right

If in principle people's Personal Information is their information, then it follows that they have the right to know precisely what information any entity currently holds about them. It also follows that they have a right to take that information – their information – to another third party if they so wish.

Its infeasible for the FTC to actively police whether all firms comply with their privacy police, and too frequently failures to comply are only discovered as a result of a breach or by the actions of a whistleblower. By requiring firms to tell individuals what information the firm collected and holds, individuals become empowered to be their own check against bad actors and confirm that the collection and use is consistent with the disclosure and consent. Individuals should also be able to receive that data in a form and format that they can then share with another entity – information collection should not be a form of product or service lock-in.

Conclusion

The FTC plays a critical role in protecting consumers across a wide spectrum of areas. Consumer data privacy and protection is the new front in the war to protect consumers from criminal bad actors and deceptive corporate practices. We believe the FTC is well-positioned today to be a global leader on privacy and we look forward to working with the agency and its leadership in protecting consumers.

Respectfully Submitted,

Virginia Lam Abrams
Senior Vice President, Communications & Government Relations

Brian Regan
Vice President, Legal, Policy, and Strategy

Starry, Inc.