Oath:

TO: The Honourable Bob Zimmer, Chair, Standing Committee on Access to Information, Privacy, and Ethics, House of Commons, Canada

FROM: Douglas R. Miller, Vice President, Privacy, and Global Privacy Leader, Oath Inc.

SUBJECT: Response to "Privacy Implications of Platform Monopolies and Possible National and International Regulatory and Legislative Remedies to Assure the Privacy of Citizens' Data and the Integrity of Democratic and Electoral Processes Across the Globe"

Mr. Chairman and Members of the Committee:

Oath appreciates the opportunity to provide for the Committee its approach to protecting consumer privacy and security for Canadian citizens using our services. We set out below how Oath provides transparency into our collection and use of data, controls for consumers, and how we protect data. We outline how digital advertising works, with particular focus on political ads and the internal protections we have in place. We close with a few thoughts on how public policy might evolve to find the right balance of ensuring consumers are protected online while also ensuring that internet and online services continue to innovate, grow and serve Canadian consumers.

Oath Inc.

Oath Inc., a wholly-owned subsidiary of Verizon formed in June of 2017, is comprised chiefly of AOL and Yahoo, along with other well-known media and technology brands around the world, such as HuffPost and Yahoo News, TechCrunch, Makers, Yahoo Finance, Yahoo Sports and Tumblr. These combined brands, digital and mobile, reach a billion people around the world.

AOL Canada and Yahoo Canada have operated in Canada for many years, currently operating as Yahoo! Canada Co. and Oath (Canada) Corp. The combined operation is based in Toronto with an office in Montreal as well, and currently employs nearly 200 people in Canada. Yahoo Canada's main businesses are Yahoo Mail (including Rogers Yahoo Mail), Search, and products such as Yahoo News, Yahoo Sports, and Yahoo Finance. Other Oath brands in Canada include AOL, HuffPost Canada and RYOT Studios.

Oath is an advertising-supported Internet business. The content people engage with on our sites – whether reading an article on HuffPost Canada, checking stock prices on Yahoo Finance or local weather on Yahoo Weather – is available without subscription or cost, thanks to advertising. In addition to a "first party" business serving the needs of visitors directly to our owned and operated sites, users of our apps, and registered members with media, content, and services, Oath has a "third party" business offering a full range of digital advertising services for advertisers, agencies and publishers. Oath's third party business, Oath Ad Platforms, is a suite of advertising and publishing solutions that makes it easier for advertisers, agencies and publishers around the world to increase their consumer engagement and revenue through Oath's trusted data, high-quality inventory, innovative ad experiences and industry-leading algorithms.

Oath Privacy Policy

At the time Oath was formed in June 2017, Yahoo and AOL initiated a company-wide integration of core assets and policies. As part of this process, Oath developed a new unified global privacy policy (https://policies.oath.com/) designed to support the integration of AOL and Yahoo. The new policy was launched to consumers in Canada in April of this year. The launch of a unified Oath privacy policy and terms of service has been a key stepping stone toward creating what's next for our consumers while empowering them with transparency and controls over how and when their data is used.

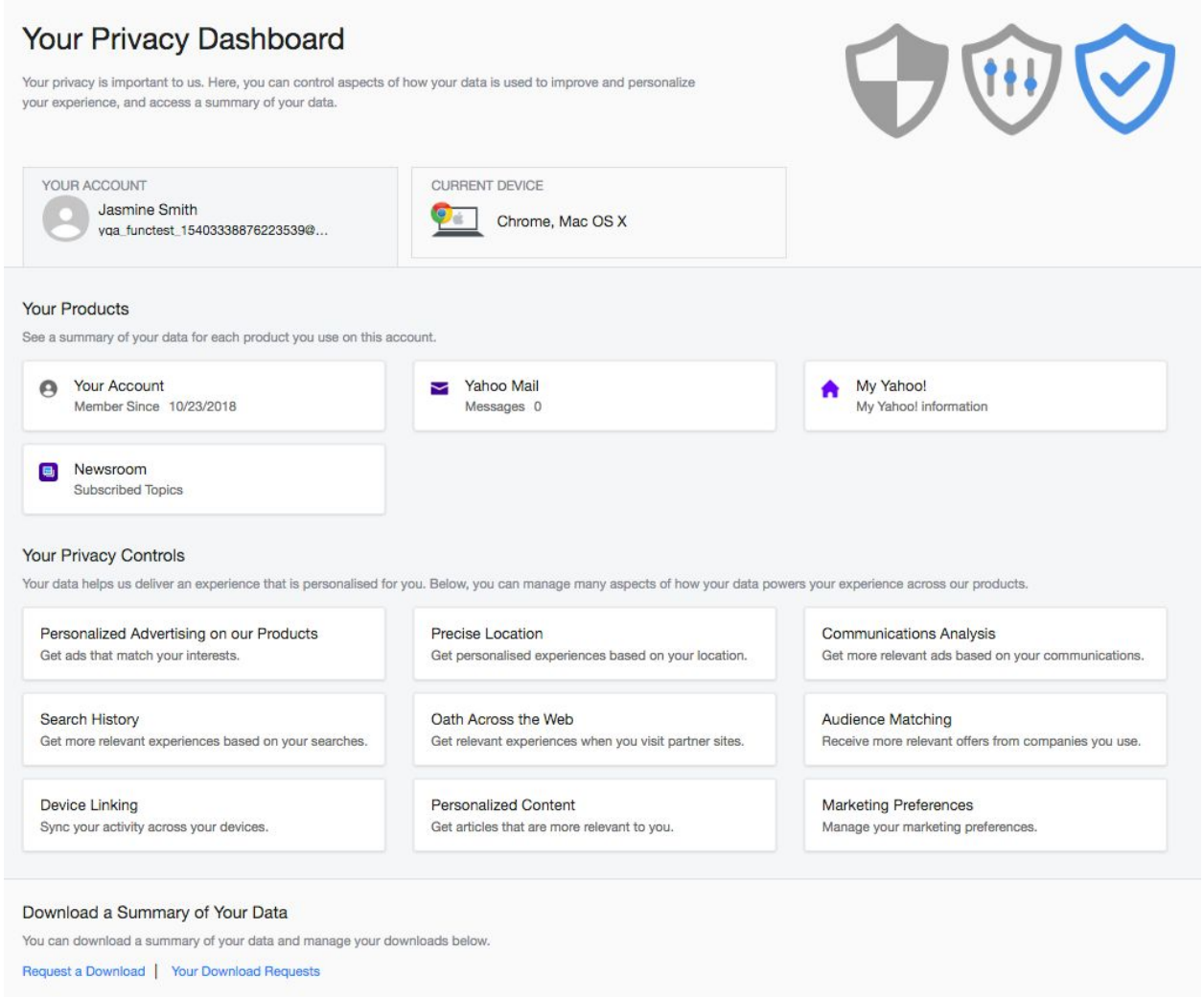
We also sought to ensure that our policies were updated to reflect new legal requirements under the EU General Data Protection Regulation and other privacy and data protection laws worldwide.

Designing for Consumers

With the launch of our new privacy policy, Oath is providing clear, transparent information and offering consumers choices related to the data that we collect and how we use it. Specifically, we designed and launched:

- **Clear, transparent consent flows:** In addition to a new policies page (https://adspecs.oath.com), Oath invested in an in-product user experience that presents users with the material changes in clear terms and asks for consent.
- **Microsite:** Oath developed a user-friendly microsite (https://mydata.oath.com) that spells out in clear terms to users how and when their data is used.
- **Integrated privacy dashboard:** A new privacy dashboard (https://policies.oath.com/us/en/oath/privacy/dashboard/) is available to users providing options for how and when their data is used across Oath's brands (*see below* for a screenshot of Oath's privacy dashboard).

Oath's Privacy Dashboard



Technical and Policy Control Mechanisms

Oath has a number of technical and policy control mechanisms to ensure ongoing governance and compliance with laws in Canada and elsewhere. Some examples include:

- Ad policies provide reasonable restrictions on allowable targeting;
- Data partnerships are protected by contractual limitations on creation of user profiles by partners;
- A Product Launch Calendar reviews material product launches for external-facing features leveraging data. Subject to established criteria, it triggers Privacy Impact Assessments;
- Technical controls include API keys, hashing/encryption of identifiers, iframes/safeframes on webpages; and

- An Internal Audit unit reviews established procedures.

Oath's Security Approach

In addition to strong privacy policies, data security is an important component of protecting consumers. Oath devotes considerable investment in security across all of our products and platforms. We employ an attacker-centric security operation, with dedicated teams engaging in continuous threat monitoring, penetration testing and investigation. Additionally, we strive for a "security by design" approach to product development and a company-wide culture of accountability.

Oath's global security effort is not just AOL and Yahoo security wired together; it's a reengineered approach to combating the most aggressive threats to user security and safety. From the strategic approach to operationalization of key security programs, Oath is differentiating itself among its peers and in the context of constantly evolving online threats.

A number of key pillars and programs operationalize this overarching approach:

- Security is baked into our company culture, where every creator, every coder and every strategist is accountable and a part of the IT Security team, known as the "Paranoids."
- We have created our own Red Team to constantly test our defenses.
- We have grown a global bug bounty program. Over 3,000 security researchers have submitted reports to our global bug bounty program over its lifetime, resulting in millions of dollars in payouts.
- Our E-Crimes Team is charged with detecting, investigating and remediating threats to our users and systems.
- We actively remediate user data in third party data dumps.
- We implement machine learning AI techniques to help detect and prevent fraudulent account access.
- We've created a hardened infrastructure through a consolidation of and investment in registration and login systems.

The threat landscape is continually evolving, and we are committed to evolve with it to keep our users secure and mitigate risk.

News, Advertising, Disinformation Campaigns and Elections

Across Oath, we are serious about ensuring the integrity of our sites.

Oath's News Properties

Oath makes significant investments in quality content – whether it's our own original journalism or journalism sourced from premium partners around the web. We have hundreds of editorial staff across Oath's news properties, including on Yahoo News, HuffPost, TechCrunch and Engadget. Our news outlets have earned many journalistic awards, including the prestigious Edward R. Murrow Award, a Pulitzer and an ASME. We take great pride in the quality of journalism on Oath's news properties. In fact, a 2017 Pew Research Center study found that Yahoo News was popular among both conservatives and progressives, with an equal number of both Trump and Clinton voters citing it as a main source of news.

Disinformation

Last fall, we uncovered 84 Tumblr accounts linked to the Russian government through the Internet Research Agency, or IRA. These accounts were being used as part of a disinformation campaign leading up to the 2016 U.S. election. The IRA-linked accounts found on Tumblr only focused on spreading disinformation in the U.S., and they were real people, not bots, who posted organic content. We did not find any indication that they ran political or issue-based ads.

After uncovering the activity, we notified law enforcement, terminated the accounts, and deleted their original posts. Behind the scenes, we worked with the U.S. Department of Justice, and the information we provided helped indict 13 people who worked for the IRA.

In addition to a public blog post announcing our findings and actions, we notified Tumblr users who engaged with these blogs. We left up any reblog chains and let Tumblr users curate their own Tumblrs using that information. We took this step because the reblog chains contain posts created by real Tumblr users, often challenging or debunking the false and incendiary claims in the IRA-linked original post.

We also took several steps to help protect Tumblr in the future. These measures include using enhanced technical solutions and human efforts to detect activity and prevent abuse of Oath platforms; continuing to participate in information sharing with our peer companies and use that collective data to find and address activity on Oath platforms; maintaining strong policies around political advertising on Oath sites; and being transparent with Tumblr's users. While our security experts are watching for signs of future activity, we believe the best defense is the public knowing how those who seek to spread disinformation operate and how to judge the content they see. To this end, we have committed to:

- Notifing Tumblr users who have liked, reblogged, replied to, or followed a propaganda account;

- Keeping a public record of usernames we've linked to IRA or other state-sponsored disinformation campaigns; and
- Alerting law enforcement.

Maintaining Strong Accountability for Political and Issue-based Advertising

While we have no indication state-sponsored actors used Oath sites for election-related advertising, we believe it is important to maintain strong policies around this type of advertising. Oath (along with Yahoo and AOL prior to Oath's formation) requires political and social issue ads include "sponsored by" or "paid for" to help users identify who placed the ad. Ads not authorized by a candidate or political party must also include contact information for the sponsoring organization. This "paid for by" disclosure must be clear and conspicuous. We prohibit ads that exploit sensitive political or religious issues for commercial gain or promote extreme political or extreme religious agendas or any known associations with hate and other activities. Additionally, all potential political and political issue advertising must be approved by the Oath Ad Policy team. Our advertising policies can be viewed at https://adspecs.oath.com/pages/oathadpolicies.

Making Advertising Relevant and Effective

An effective advertisement is targeted to the right consumer or audience at the right time. Advertisers, publishers, and ad tech companies are each interested in ensuring that consumers receive relevant ads and – importantly – that many more consumers do not receive irrelevant ads. Similarly, when a relevant ad is served, advertisers get more value from their advertising investments, publishers generate the revenue that allows them to invest in new and compelling content, and consumers receive ads relevant to their interests. Oath serves a variety of ads on its owned and operated properties as well as on its third party publisher network.

Ad targeting can be controlled by users in a variety of ways. Companies like Oath that embrace and support industry self-regulation require that the other companies in their ad networks are contractually bound to provide appropriate notice to consumers of how data is collected and used, including enhanced notice for ads, provide a link to opt outs from interest-based ads, honor limit ad tracking signals, and ensure reliable sources for onboarded data. The Network Advertising Initiative has added requirements for ensuring opt out control for non-cookie-based tracking as well. Self-regulation is not a panacea for online privacy, but it helps ensure an ecosystem of cooperative compliance. Oath supports industry self-regulation for digital advertising, such as the Digital Advertising Alliance Canada, the Network Advertising Initiative and the Digital Advertising Alliance in the U.S., and the European Digital Advertising Alliance in the EU.

How data supports free content online

There has been much recent debate about the data that some companies have and their stewardship of that data. We think these are the right questions for both consumers of free online services as well as policymakers to ask. As these dialogues are ongoing in this Committee and elsewhere around the world, we offer four points for consideration.

First, advertising drives commerce. Economic prosperity has always been aided by advertising. Data and ad technologies are tools, which can be used responsibly to strike the balance between commerce and respect for privacy.

Second, although online data gets a lot of attention because of the scale and name recognition of huge companies, online data is generally collected with more notice and available choice than much of the offline data now available for onboarding. The average storefront retailer has names, addresses, phone numbers, purchase histories, and credit card numbers at hand. Data brokers gather vast amounts of data – much of it from publicly available sources – and render sophisticated modeling techniques before selling such data across the ad ecosystem. We support appropriate privacy protections for consumers, and we believe such protections should be required by all actors in the economy, not just online actors.

Third, online publishers are able to provide diverse, fresh and compelling content when they can generate the revenue to invest in such content. Advertising makes that possible. Mere context-based targeting, or advertising based on the content of the website, simply does not generate adequate revenue, but well-targeted ads do. With respect to news sites in particular, digital advertising preserves, free for consumers, the marketplace of ideas essential for an informed electorate.

Fourth, the evolution of privacy law should look to the future, and the future brings the Internet of Things, artificial intelligence, and machine learning. Consent may not be a scalable solution as people around the world connect more and more devices to the internet. The collection of data becomes harder to prevent and less desirable when data drives artificial intelligence and machine learning. An informed perspective on privacy and security, alongside legal frameworks that support sound data governance and accountability are a solid foundation for consumer privacy as technology evolves.

Elements of Evolving Privacy Law

There has been much discussion of evolving privacy laws with the EU's General Data Protection Regulation and other laws that will enter into force in the coming months. While the GDPR contains many welcome elements, including enhanced requirements for governance and accountability, some

ambiguities have emerged in its language and interpretation by regulators. Regulation should be easy for consumers and for regulated entities to understand. It should be robust, technology- and business model-neutral for the protection of privacy and personal data that advances the interests of all stakeholders, including consumers, businesses, individuals and governments.

Along with our parent company, Verizon, Oath subscribes to a set of broad objectives that we believe should inform the evolution of privacy regulation on the internet.

- Consistency. One set of rules for all industry sectors.
- Flexibility. With respect for the sensitivity of data, frameworks should be flexible so they do not quickly become outdated.
- Transparency. Companies must provide clear and easy to understand information about their practices with data.
- Choice. Companies must provide consumers with the opportunity to opt in to collection, use and sharing of sensitive information and opt out of the collection and use of personal information, with appropriate exceptions for legitimate operational and other uses, such as anti-fraud or legal process.
- Data Security and Breach Notification. Companies should have reasonable security protections in place.
- Safe Harbor Programs. A safe harbor program could provide clarity that companies can follow and know that they are compliant.
- Enforcement. In the U.S. we recommend Federal Trade Commission enforcement as well as enforcement by state Attorneys General. In Canada, enforcement by the Office of the Privacy Commissioner would be appropriate.

Oath is grateful for the opportunity to provide these comments to inform your development of policies that enhance personal data protection, further the trust relationship between companies and their consumers, and enable innovation while also avoiding regulatory fragmentation that undermines all three of these goals[1]. We would be pleased to answer any further questions the Committee may have.

[1] Oath is a member of the Information Technology Industry Council (ITI), a global trade association of the technology sector. Oath supports ITI's Framework to Advance Interoperable Rules (FAIR) on Privacy, a robust, technology and business model-neutral roadmap that advances the privacy rights of consumers and defines the responsibilities of companies in using personal data while continuing to enable innovation.