Questions for the Record

House of Representatives Subcommittee on Consumer Protection and Commerce of the Committee on Energy and Commerce

Hearing on *Protecting Consumer Privacy in the Era of Big Data*

David F. Grimaldi, Jr., Executive Vice President, Public Policy, Interactive Advertising Bureau

The Honorable Robin L. Kelly:

In the wake of the repeal of broadband privacy rules last year, what are your thoughts on privacy proposals including ISPs. For example, should ISPs be able to mine DNS data? Are there any other solutions to this that could protect consumers from these privacy violations if we don't come up with a regulatory one?

Consumers want strong privacy protections that apply consistently to their data across the Internet, regardless of what state they happen to be in or what entity is holding the data, as evidenced by a Peter Hart survey confirming that 94% of consumers want the same protections to apply to their online information regardless of the company that collects or uses it.[1]

ISPs should of course be included in any federal privacy legislation, but a cornerstone of federal legislation should be that there are consistent obligations imposed on all entities that collect and use consumer data.

ISPs have made a number of enforceable public commitments not to sell or monetize sensitive user data without express customer consent, and to be transparent with their customers regarding how their information will be used, shared, protected.[2][3]

At the same time, ISPs need to access and use information like DNS information to deliver their services, to keep their networks and users secure, and to improve their services and develop new ones. A law that follows the basic principles I set forth in my testimony before the Committee – focusing on the risk of harm to the consumer and not on the identity or business model of the marketplace participant – is the best way to ensure that any problematic practices are prohibited, while allowing pro-consumer, pro-privacy practices to flourish.

Companies understand the importance of privacy to consumers, and they are working on a number of different fronts – including through open standards organizations – to identify ways to improve privacy and security standards, which they can then integrate into their products and services regardless of the

---

[1] https://www.progressivepolicy.org/issues/economy/ppi-poll-recent-national-survey-internet-users/
[2] https://api.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf
[3] https://www.ncta.com/positions/isp-privacy-principles

regulatory regime. With respect to DNS, for example, the Internet Engineering Task Force (IETF) – the premiere organization for developing the standards that serve as a technical foundation of the Internet – recently developed two new DNS protocols -- DNS over TLS and DNS over HTTPS -- that will enable the encryption of DNS queries. ISPs are currently examining these new protocols to determine whether, and, if so, when and how to deploy them.

The Honorable Richard Hudson:

Mr. Grimaldi, in your testimony you highlight that small businesses and startups have seen the negative impacts of GDPR. Have companies exited Europe because of GDPR? If so, can you please explain why that is and what we can do to ensure we maintain a regulatory environment in the U.S. that allows businesses to grow?

Following the implementation of the GDPR, many U.S.-based companies and publishers chose to exit the European market instead of risk the significant fines related to potential GDPR violations.

Jeff South of the Nieman Foundation for Journalism at Harvard University reported that nearly one out of three of the 100 largest U.S. newspapers were no longer available in Europe more than two years after the law was passed.

The decision to exit the European market has not been confined to large U.S. publishers. As of March 20, 2019, 1,129 U.S. websites, including many small newspapers and online services, are still unavailable in the European Union following the implementation of GDPR.[4] This includes companies such as The Fayetteville Observer, North Carolina's oldest newspaper which traces its roots back to 1816.[5][6]

Additional evidence suggests that the negative impact of GDPR has been most acutely felt by smaller U.S. businesses. In the digital advertising industry, one study has indicated that smaller advertising companies have lost between 18 percent to 31 percent in market share since GDPR went into effect, while market leaders have gained in reach over that same period.[7]

While well intentioned, we believe GDPR imposes significant burdens on businesses while failing to stop many practices that are truly harmful. Furthermore, GDPR fails to recognize the various ways in which digital advertising subsidizes the plentiful, varied, and rich digital content and services consumers use on a daily basis and have come to expect.

IAB recommends that as an alternative to GDPR, a new U.S. federal privacy law should impose clear prohibitions on a range of harmful and unreasonable data collection and use practices specifically identified in the law. Furthermore, such a law should distinguish between data practices that pose a threat to consumers and those that do not, rather than taking a broad-brush approach to all data collection and use.

---

[4] https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr
[5] https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr
[6] https://www.fayobserver.com/about_us
[7] https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr

In this way, we believe the U.S. can provide meaningful protections to all Americans while ensuring U.S. businesses of all sizes and across all industries are able to compete and grow.