JOHN M. SHIMKUS
15TH DISTRICT, ILLINOIS

2217 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-5271

ENERGY AND COMMERCE COMMITTEE
SUBCOMMITTEES:
ENVIRONMENT AND THE ECONOMY
CHAIRMAN
HEALTH
ENERGY AND POWER
COMMUNICATIONS AND TECHNOLOGY

Congress of the United States
House of Representatives
Washington, DC 20515–1315

May 11, 2018

15 PROFESSIONAL PARK DRIVE
MARYVILLE, IL 62062
(618) 288-7190

CITY HALL, ROOM 12
110 EAST LOCUST STREET
HARRISBURG, IL 62946
(618) 252-8271

101 NORTH FOURTH STREET, SUITE 303
EFFINGHAM, IL 62401
(217) 347-7947

201 NORTH VERMILION STREET, SUITE 218
DANVILLE, IL 61832
(217) 446-0664

Mr. Larry Page
Chief Executive Officer
Alphabet, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Page:

Since arriving in Congress, we have strived to help make the internet a competitive, open and safe place and are gratified to have seen it become a tremendous resource for all Americans and the businesses they support. Sadly, however, we have all witnessed how this amazing technological achievement can also be used to perpetrate criminal and other illicit behavior, which compromises our public safety and security, and undermines the very foundation of this indispensable platform.

The solution to protecting the integrity of the internet is, of course, transparency and public accountability. It is transparency that has driven one of the core ingredients of a sustainable internet, the publicly accessible WHOIS database. The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the WHOIS database, and contractually requires registrars and registries to make public certain WHOIS data regarding the identity of domain name registrants, including name, email, and phone number. WHOIS serves as the backbone of consumer trust and online protection because it provides the public with an indispensable window into who owns and operates websites in which we place our trust and, in some cases, personal information.

From its founding, the WHOIS database was designed as a public directory to allow anyone to contact any individual who has obtained an internet domain address. Domain name registrants have long been aware that they must provide certain identifying information that will be publicly disclosed, and that such information may be used for matters of public safety, consumer protection, dispute resolution, and enforcement of rights. However, ICANN has unfortunately recently proposed changes to the publication of WHOIS data that will dramatically alter its essential and historical purpose and do not do justice to the spirit of the European Union's impending General Data Protection Regulation (GDPR).

We write to express concern that the interim ICANN proposal removes access to even the most basic of WHOIS information, which is not a reflection of the requirements of the GDPR. Restricting such access to WHOIS data would diminish online transparency, responsibility, and accountability, as well as jeopardize internet security and safety. Moreover, it would frustrate what ICANN itself has identified as WHOIS's most basic public policy interests, including "enhancing trust in the DNS, ensuring consumer protection, protecting intellectual property, combating cyber-

crime, piracy and fraud."[1] Of course, it would also thwart even preliminary examinations into identity theft, cyber-attacks, unlawful sale of drugs, human trafficking, and other criminal behavior. Relying on an overly broad interpretation of the GDPR could have the perverse consequence of jeopardizing consumer safety and the ability of the public to identify who owns and operates internet domain addresses (and, by extension, who then collects user data via said domain).

We serve on the U.S. House of Representatives Committee on Energy and Commerce, which regularly conducts significant oversight of NTIA, ICANN, the domain name ecosystem, and the IANA transition. In 2015 the House passed the DOTCOM Act, which Mr. Shimkus authored, and as such we believe it is imperative that registrars and registries, together with others in the ICANN community, work with NTIA to ensure there is balanced progress in developing a GDPR-compliant accreditation framework that preserves accountability by allowing qualified access to registrant information.

We respectfully request that you respond promptly in writing to the following:

1. Please clarify what GDPR-related changes you have made or intend to make with respect to the WHOIS data you collect or receive;
2. Please indicate whether, with the exception of registrants who are natural persons and confirmed residents of the EEA, you will continue to publish in a publicly accessible WHOIS directory all domain registrant data that your current contracts with ICANN (under the Registrar Accreditation Agreement or the applicable Registry Agreement) require to be collected and made public—even if doing so requires you to reverse changes you have already made or are preparing to make;[2] and
3. Please confirm that you are actively working in good faith with others in the ICANN community (such as public safety non-governmental organizations, cyber-security professionals, and intellectual property owners) to launch—before any WHOIS data is removed from public access—a GDPR-compliant accreditation framework that allows qualified access to such information for legitimate purposes.

Sincerely,

The Hon. John Shimkus
Member of Congress

The Hon. Raul Ruiz
Member of Congress

[1] See ICANN's Governmental Advisory Committee (GAC) March 15 ICANN 61 communiqué, reflecting a formal consensus view of its more than 170 member countries and economies.

2 We are aware that some of your domain name registrants currently subscribe to privacy or proxy registration services that mask some of their WHOIS data from unfettered public access. The inquiry we are making is without prejudice to the continued operation of such services in accordance with your existing ICANN contractual obligations, including the implementation of ICANN policies governing the minimum terms and conditions under which such masked data would be published or disclosed to qualified investigators, law enforcement, and similar requestors.