Response to Written Questions Submitted by Hon.
Roger Wicker
Written Questions for the Record to
Dr. Roslyn Layton

Question 1. Dr. Layton, it seems that the stated intention and scope of the recent EU General Data Protection Regulation (GDPR) is far different from the impacts of its implementation. Can you comment on how the GDPR has been implemented as it relates to access to WHOIS data, which is critical to the security and safety of the open internet itself?

Response. The July 31st hearing established that the stated intention and scope of the GDPR is far different from its implementation. To begin, Americans have different conceptions of privacy and data protection compared to Europeans. Moreover, the process to make the respective regimes, move in the opposite directions. Americans may have a starting point of privacy, a deductive process from which data protection policy and regulation flows. The Europeans on the other hand, are inductive. They build a series of data protection regulations, and that resulting corpus is what is referred to as privacy. The GDPR itself only mentions "privacy" in three instances, and it is more correctly understood as a model of data governance, rather than privacy.

Moreover, the GDPR has many unintended consequences, one of which is the undermining of the transparency of the WHOIS query and response protocol as it needed by law enforcement, cybersecurity professionals and researchers, and trademark and intellectual property rights holders.[1] The problem is best described as the conflict between the right to be informed and the right to be forgotten.[2] It can also be understood within the context of the problem of "privacy overreach,"[3] in which the drive to protect privacy becomes absolute, lacks balance with other rights, and unwittingly brings worse outcomes for privacy and data protection.[4] The situation harkens back to a key fallacy of so-called privacy activists who attempted to block the rollout of caller ID because it violated the privacy rights of intrusive callers. Today we agree that the receivers right to know who is calling is prioritized over the caller.[5] Similarly we can understand that the needs of public safety will supersede data protection, particularly in situations of danger to human life. Moreover, we should at least expect intellectual property to be in balance with data protection, not in the conflict we find it today with the GDPR.

---

[1]Shane Tews. "How European data protection law is upending the Domain Name System." American Enterprise Institute. February 26, 2018. https://www.aei.org/publication/how-european-data-protection-law-is-upending-the-domain-name-system/

[2] Shane Tews, "Privacy and Europe's data protection law: Problems and implications for the US". AEI.org May 8, 2018. http://www.aei.org/publication/privacy-and-europes-data-protection-law-problems-and-implications-for-the-us/

[3] *See* Justin "Gus" Hurwitz and Jamil N. Jaffer, "Modern Privacy Advocacy: An Approach at War with Privacy Itself?, Regulatory Transparency Project of the Federalist Society," June 12, 2018, https://regproject.org/paper/modern-privacy-advocacy-approach-war-privacy/.

[4] See Maja Brkan, *The Unstoppable Expansion of the EU Fundamental Right to Data Protection*, *Maastricht Journal of European and Comparative Law* 23, no. 5 (2016): 23, http://journals.sagepub.com/doi/abs/10.1177/1023263X1602300505?journalCode=maaa.

[5] Supra Hurwtiz

While the goal of the GDPR may have been data protection, an overbroad application by registrars and registry operators is threatening to jeopardize the safety of internet users and the security of the internet generally, both within the EU and beyond its borders. From its launch, WHOIS was designed to enable people to identify whom they are dealing with on the other side of a web site. This not only promotes the trust necessary to facilitate online commerce, but is also critical for public safety, consumer protection, law enforcement, dispute resolution, and enforcement of rights.

The Internet Corporation for Assigned Names and Numbers, however, announced a Temporary Specification recently that allows registries and registrars to obscure WHOIS information they were previously required to make public, ostensibly in order to comply with the GDPR.[6] This will hinder efforts to combat unlawful activity online, including identity theft, cyber-attacks, online-espionage, theft of intellectual property, fraud, unlawful sale of drugs, human trafficking, and other criminal behavior, and is not even required by the GDPR, as the U.S. Departments of Commerce and Homeland Security, the National Telecommunications and Information Administration, and ICANN's own Governmental Advisory Committee of more than 170 member countries and economies have all observed.[7]

Notably the GDPR does not apply at all to non-personal information and states that disclosure of even personal information can be warranted for matters such as consumer protection, public safety, law enforcement, enforcement of rights, cybersecurity, and combating fraud. Moreover, the GDPR does not apply to domain names registered to U.S. registrants by American registrars and registries. Nor does it apply to domain name registrants that are companies, businesses, or other legal entities, rather than "natural persons."

To protect American citizens, Congress therefore might consider urging—both through its own diplomatic channels and in its work with the White House and federal agencies—that European policymakers clarify that the GDPR does not prevent access to WHOIS data for law enforcement, consumer protection, and rights enforcement. Congress might also indicate to domain name registries and registrars that it expects them to continue making WHOIS data publicly available to both law enforcement and private entities for purposes of protecting U.S. consumers and rightsholders. Federal legislation requiring such disclosure also should be considered to ensure that the European directive does not inappropriately interfere with U.S. prerogatives to set U.S. policy and protect its citizens.

Congress should take note of some key actors driving the GDPR whio are now in key political positions in the EU. Notably the coming conflict between the GDPR and WHOIS was described highlighted in a 2017 academic article by law and computer science researchers at the University

---

[6] ICANN, TEMPORARY SPECIFICATION FOR GTLD REGISTRATION DATA (adopted May 17, 2018), https://www.icann.org/resources/pages/gtld-registration-data-specs-en.

[7] *See* U.S. DEPT. OF COMMERCE AND U.S. DEPT. OF HOMELAND SECURITY, A REPORT TO THE PRESIDENT ON ENHANCING THE RESILIENCE OF THE INTERNET AND COMMUNICATIONS ECOSYSTEM AGAINST BOTNETS AND OTHER AUTOMATED, DISTRIBUTED THREATS 23, 24 (May 2018), https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf; Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, ICANN 61 (March 12, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61; ICANN, GOVERNMENTAL ADVISORY COMMITTEE, *Communiqué—San Juan, Puerto Rico* (March 15, 2018), https://gac.icann.org/advice/communiques/20180315_icann61%20gac%20communique_finall.pdf.

of Vienna.[8] Austria has been ground zero for GDPR activism. The current head of the EU Data Protection Supervisor (EDPS), Andrea Jelinek, was formerly the chief of the Austrian Data Protection Authority which worked closely with Austrian privacy activist Max Schrems. Schrems founded the Vienna-based non-profit None of Your Business (NOYB) to professionalize GDPR litigation and has lodged GDPR complaints against Google and Facebook, requesting some $8.8 billion in damages on the day the GDPR came into effect.[9] Jelinek has incorporated NOYB parlance into EDPS activities and policy arguments.[10] In her role in the Article 29 Working Party, the group that drove the promulgation of the GDPR, Ms. Jelinek noted that the elimination and masking of WHOIS information is justified under the nebulous, overbroad, and invented conceptions of the GDPR.[11] It is understandable that is group of GDPR supporters are willing to torpedo internationally accepted norms and conventions in order to legitimize the GDPR.

My testimony underscores that the GDPR violates many US laws and norms and is likely illegal under international law and should be challenged by US policymakers.

[8] Erich Schweighofer, Vinzenz Heussler, and Walter Hötzendorfer. "Implementation Issues and Obstacles from a Legal Perspective." Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level. Editor Florian Skopnik. Taylor & Francis, 2017. https://www.taylorfrancis.com/books/e/9781315397894

[9] https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf

[10] See the discussion of "forced consent", a term defined by NOYB which has been co-opted by the EDPS.

[11] https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf

Response to Written Questions Submitted by Hon.
Roy Blunt
Written Questions for the Record to
Dr. Roslyn Layton

Question 1. As you know, liability protections for online platforms were instituted, in part, so that they could filter harmful and illicit content without the threat of civil litigation. In recent years, however, digital piracy and other illegal digital transactions have been on the rise, and most of the activities to counter it have been retrospective. In your testimony, you state that technology and business models are improving in a way that could better detect pirated, unlicensed content, yet tech companies do not appear to be effectively vetting and filtering content on a proactive basis – even that which is clearly illegal. In 2017, there were an estimated 22.9 billion visits to streaming piracy sites worldwide across both desktops and mobile devices, a 39 percent increase over the comparable figure for 2016. Considering the rise of illegal traffic over online platforms:

- Do you believe that technology companies are doing enough to curb the spread of illicit material online?

- Do you believe that the liability protections for technology companies as currently enacted are accomplishing their intended goal?

Response. The presumption some 20 years ago behind section 230 of the Communications Act and Section 512 of the Copyright Act was that with liability protections, online platforms would take proactive steps to combat illegal activity over their services. Moreover, those protections were only meant to accrue to entities that were not profiting from illegal activity. Unfortunately, many platforms are primarily taking steps after-the-fact (if at all), once harm as already occurred, rather than proactively curbing abuse of their systems. Moreover, because many platforms' business models are rooted in advertising or the commercialization of data related to internet users' online behavior, some platforms generate revenue from illicit online behavior. Clearly this was not the intent of the liability shields, and many online platforms can and should be doing more.