FACEBOOK

1 Hacker Way
Menlo Park, California 94025
United States of America

September 2, 2020

The Honorable Adam Candeub
Acting Assistant Secretary of Commerce for Communications and Information
Herbert C. Hoover Building
U.S. Department of Commerce
National Telecommunications and Information Administration
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

Re: Additional Information Regarding WHOIS

Dear Adam,

Thank you for taking the time last month to listen to industry stakeholders regarding the importance of WHOIS and the problems we've identified with the ICANN policy proposals for a new system of WHOIS access.

I'm following up on your request for additional information regarding this topic, and its continued importance to Facebook.

- WHOIS information and access is critical to protect the Facebook family of products from cybersecurity threats and fraud. Ensuring that WHOIS data is accurate, uniform, and easily accessible is key to our efforts to identify bad actors that target our platform and users with things like fake news, phishing attacks, brand infringement, and other malicious activity.
- WHOIS is also important to ensure transparency and accountability on the Internet across the globe. WHOIS helps build an ecosystem of trust and security that not only impacts Facebook users, but supports the billions of users worldwide that rely on the Internet to engage in commerce, use social media to stay connected, and build communities.
- The usefulness of the WHOIS system has been significantly impaired since 2018. We no longer have meaningful, timely access to WHOIS as an investigative tool to identify bad actors and domain names involved in cybersecurity threats. Facebook now encounters significant delays and denials of access when requesting WHOIS, even in clear-cut cases of phishing, fraud and trademark infringement. This overall unavailability of WHOIS (with an

over 70% denial rate) has made our efforts to fight these types of abuses much more difficult.[1]

- The problem continues unabated in the face of increased abuse related to COVID. In the first few months of the COVID crisis, Facebook responded with a targeted, global enforcement effort (for abuse outside of Facebook's platforms) to stop bad actors from harming our users and platforms during the pandemic. We identified over 3500+ phishing campaigns involving our brands and COVID-related matters, responded to over 600 potentially infringing/fraudulent off-platform COVID social media entries, over 250 fraudulent/infringing COVID domain names, and defensively registered over 1000 domain names containing our major brands and COVID-related terms across the key top-level domains to help pro-actively block virus-related abuse. Yet despite our efforts to address this abuse quickly, we were routinely denied WHOIS access for COVID related DNS abuse.
- It's been over two years since ICANN convened the expedited policy process known as the EPDP to resolve this issue. Unfortunately, this is not an issue that is capable of being fixed by ICANN through its multi-stakeholder model and policy processes. If adopted, ICANN's proposed access system would repeat today's broken WHOIS system where very few legitimate requests actually result in disclosure. Moreover, the lack of automated responses, even in obvious cases of phishing, fraud and trademark abuse, will result in significant delays to mitigation efforts, when quick action is critical to prevent massive consumer harm.

I hope this gives you a better understanding of Facebook's perspective on this important topic. Please feel free to reach out to me if you have any questions or would like additional information.

All the best,

Margie Milam
Intellectual Property & DNS Policy Lead
Facebook, Inc.

[1] Our experience is not unique among technology companies. For examples, please see the statement by the Cybersecurity Tech Accord on November 30, 2018 describing several compelling examples of the challenges faced by member companies in mitigating cybersecurity threats in the absence of WHOIS.