ROBERT E. LATTA
5TH DISTRICT, OHIO

DEPUTY WHIP

COMMITTEE ON
ENERGY AND COMMERCE

SUBCOMMITTEE ON
COMMUNICATIONS AND TECHNOLOGY
REPUBLICAN LEADER

SUBCOMMITTEE ON ENERGY

SUBCOMMITTEE ON CONSUMER
PROTECTION AND COMMERCE

Congress of the United States
House of Representatives
Washington, DC 20515–3505

WASHINGTON OFFICE:
2467 RAYBURN HOUSE OFFICE BUILDING
(202) 225–6405

DISTRICT OFFICES:
1045 NORTH MAIN STREET
SUITE 6
BOWLING GREEN, OH 43402
(419) 354–8700

101 CLINTON STREET
SUITE 1200
DEFIANCE, OH 43512
(419) 782–1996

318 DORNEY PLAZA
ROOM 302
FINDLAY, OH 45840
(419) 422–7791

June 24, 2020

The Honorable William Barr
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable Christopher Wray
Director
Federal Bureau of Investigations
U.S. Department of Justice
935 Pennsylvania Avenue, NW
Washington, DC 20535

The Honorable Timothy Shea
Acting Administrator
Drug Enforcement Administration
U.S. Department of Justice
8701 Morrissette Drive
Springfield, VA 22152

Dear Attorney General Barr, Director Christopher Wray, and Acting Administrator Shea,

I write to request information about how the Department of Justice, the Federal Bureau of Investigations (FBI), and the Drug Enforcement Administration utilize domain name information, also known as WHOIS, in carrying out its obligations to conduct investigations and intercede when illegal activity has been identified, particularly online.

Since the outbreak of the COVID-19 pandemic, we have seen a tremendous increase in online fraud targeting consumers. In a press release dated April 1, the FBI noted that it, "… anticipates cyber actors will exploit increased use of virtual environments by government agencies, the private sector, private organizations, and individuals as a result of the COVID-19 pandemic."[1] Later that month, the FBI noted it was able to, "disrupt hundreds of internet domains used to exploit the COVID-19 pandemic to commit fraud and other crimes."[2] Clearly, there is a need to be vigilant and deploy all the tools at our disposal to identify illegal operations and act when necessary.

[1] "Cyber Actors Take Advantage Of Covid-19 Pandemic To Exploit Increased Use Of Virtual Environments". Federal Bureau of Investigation. https://www.ic3.gov/media/2020/200401.aspx April 1, 2020.
[2] "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams". Federal Bureau of Investigation. https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams April 22, 2020.

PRINTED ON RECYCLED PAPER

A number of consumer, public health, and cybersecurity groups have voiced concerns that the recent implementation of the European Union's General Data Protection Regulation (EU GDPR) has had a negative impact on the ability of law enforcement, third-party organizations, and others to identify bad actors online.[3] I am interested in your observations since the EU GDPR went into effect in May of 2018. Specifically, please provide me information as to:

- If and how your office uses or has used WHOIS in the execution of its functions?
- If and how your office has experienced increased difficulty (including delays) in accessing WHOIS information since the May 2018 implementation of the EU GDPR?
- If and how your office would be able to more effectively conduct investigations and/or intercede in illegal activity with greater WHOIS access?

Thank you for your attention to this important matter. I would appreciate a response to these questions by July 31, 2020. If you have any questions, please contact Rachel Rathore on my staff at 202-225-6405.

Sincerely,

Robert E. Latta
Member of Congress

[3] Letter to Vice President Mike Pence. https://secureandtransparent.org/wp-content/uploads/2020/04/Letter-to-VP-Pence-re-COVID-19-Scams-4-9-20.pdf April 9, 2020.