July 12, 2018

U.S. House of Representatives
Energy and Commerce Committee
Subcommittee on Communications and Technology
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Blackburn and Ranking Member Doyle:

My name is Garth Bruen and I am contacting you in reference to what is known as the WHOIS system, the record set that underlies the Internet. As Congress continues to consider NTIA reauthorization I would request that certain facts be included in the discussion. The ability to quickly identify a party behind illicit activity is paramount to ensuring public safety and commercial transparency. Yet this ability is being rapidly degraded with intent. I have just participated, by invitation of Commissioner Gottlieb, in the FDA Opioid Summit. There, I presented the findings of research concerning the online availability of narcotics. None of this research involved the so-called "dark web" but rather focused on the common open Internet. As horrible as Internet opioid traffic is, it is only one of a myriad of ways our network is abused at great cost to us all. The Internet is a crucial modern innovation, but the Domain Name System is also a weapon pointed at consumers and businesses with relative impunity. Understand that all Internet viruses, spam, phishing and network intrusions are sourced at secretly owned domain names. There is an entire illicit economy that depends on transparency failure as a tool.

I am the author of *WHOIS Running the Internet* which is the result of ten years of research on the subject. WHOIS was intended from the beginning to provide transparency into a system that can be accessed (and abused) by anyone. As such, the Internet is a public space and WHOIS exists to create responsibility through commercial identity. If malicious actors were truly required to identify themselves they would not purchase domain names for their various attacks.

It is stated in the draft legislation that: *"ICANN maintains and enforces contracts with all registrars, requiring them to continue to collect identifying information from registries during the domain registration process".* In practice this is a failure. By-and-large registrars are not collecting or providing data and ICANN is not properly enforcing their contracts. As a former elected At-Large advisor to ICANN I am able to say with certainty that consumer protection and user safety are not priorities of the organization. This has been regularly stated by executive ICANN staff and ICANN board members. As a matter of core philosophy Internet users are not constituents of ICANN, only the narrow commercial domain name entities are recognized stakeholders. As an issue of policy ICANN's relationship with Registries and Registrars supersedes any obligation to the public.

The malicious actors are expected to self-report data to the registrars. So, the parties who have everything to lose by being identified are the same ones who ultimately control the record data. Collection of such data by contracted parties generally impedes profit to those companies and in turn reduces fees to ICANN itself. So in practice the process is bypassed. This is a perverse relationship which has become normalized over two decades. It is a situation that would be intolerable with automobiles, real estate, business licensure, or any other transaction that occurs within a public space. We have an expectation, for example, when riding a bus that the

driver, system operator and vehicle manufacturer can easily be identified. This kind of basic reason is being erased on the Internet.

The new European GDPR, if used properly, should protect consumers but it is being misapplied by some U.S. Internet companies to add secrecy to commercial activity. While it is true there are grave and serious threats to individual privacy on the Internet, this concern is being shoehorned into commercial space, especially the illicit. The mass data breach incidents that created a need for GDPR standards were in fact executed by the same bad actors who would benefit from further secrecy.

The bottom line is that the system requires more attention and oversight than has been the standard since it was originally implemented. The self-reporting and self-policing policies are not working as expected. I encourage Congress to take this all into consideration. I am at your disposal if further information is needed and appreciate your efforts on this issue.

Sincerely,

Garth Bruen, WHOIS Policy Researcher