Public Submissions

1. Josh Andrews
2. Carlos Carpi
3. Naor Gozlan
4. Briar Greenway
5. Heather Houser
6. Dean Marks
7. Kahari Nash
8. Tarlochan Rangi
9. Noble Shih
10. John Wickizer
11. John Wickizer #2
On behalf of the Coalition for a Secure & Transparent Internet (CSTI), we appreciate the U.S. Federal Trade Commission’s (FTC) ongoing efforts to protect consumers and its open meeting to discuss Identify Theft and Available Resources for Consumers. CSTI believes that the restoration of WHOIS domain name registration information is critical to any efforts to improve consumer protection, combat identify theft and improve cybersecurity across the board.

CSTI was founded in 2018 by a diverse set of stakeholders brought together over the loss of WHOIS data as a result of an overly broad interpretation of the European Union’s General Data Protection Regulation (GDPR). Our members include individuals and organizations focused on illegal online pharmaceutical sales, human and sexual trafficking, cybersecurity, online fraud as well as the protection of intellectual property.

WHOIS information is a critical tool in identifying who is behind a domain name or website. This information has been a public safety tool used for accountability in the protection of consumers on the Internet from all types of fraud and counterfeited products, in the development of cybersecurity measures and in halting sexual trafficking and exploitation. Moreover, WHOIS information enables law enforcement and investigators to connect malicious actors to one another and preemptively stop harmful activity.

In an overbroad and misapplied response to the European Union’s General Data Protection Regulation (GDPR), since 2018 domain name registries and registrars globally have systematically shut down access to WHOIS data. This result is merely commercially convenient for registries and registrars, not required by the EU law. In the two years since implementation of the GDPR, the internet has gotten darker, less transparent, and less safe for individuals and businesses alike. As a recent study concerning cybersecurity indicates, this lack of access to WHOIS data “continue[s] to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyberattacks.”

The lack of the access to WHOIS data has negative implications for a variety of public interests, including but not limited to:

- Online shopping and sales,
- Illegal online sales of medicines and controlled substances,
- Online fraud and sales of counterfeit products,
- Cybersecurity,
- Anti-human trafficking and anti-sexual exploitation, and
- Intellectual property protection,

The rise in internet crime is serious and alarming. In March 2021, the FBI’s Internet Crime Complaint Center releases its 2020 Internet Crime Report. The report includes information from 791,790 complaints of suspected internet crime—an increase of more than 300,000 complaints from 2019—and reported losses exceeding $4.2 billion.

Last year, several Executive Branch agencies responded to an inquiry from Congressman Latxa (R-OH) as to the role WHOIS plays in their investigative and enforcement obligations, how the loss of access to this information has critically impeded those efforts and whether they would be able to better carry out those obligations with restored access to WHOIS.
In its response to Rep. Latta, the Federal Trade Commission noted, “Before the GDPR took effect in May 2018, the FTC and other consumer protection and law enforcement agencies routinely relied on the publicly available registration information about domain names in WHOIS databases to investigate wrongdoing and combat fraud.” Other agencies shared the FTC’s view:

- The U.S. Food & Drug Administration stated, “Access to WHOIS information has been a critical aspect of FDA’s mission to protect public health. Implementation of the EU’s General Data Protection Regulation has had a detrimental impact of FDA’s ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients.”

- The U.S. Immigration and Customs Enforcement Homeland Security Investigations (HSI) and the National Intellectual Property Rights Coordination Center (IPR Center) indicated, “HSI uses domain name registration information, previously available via online WHOIS query, to aid in the identification of persons or entities responsible for registering domains that are used to conduct a wide variety of crimes, which include intellectual property crimes, cyber-crimes (such as theft of personally identifiable information [PII] and credit card information), crimes related to illegal importation and exportation of goods, and the promotion and distribution of child sex abuse material.”

Congress is also on record supporting accessible WHOIS information. Last year’s Consolidated Appropriations Act for 2021 (P.L. 116-260) provided that:

“NTIA is directed, through its position within the Governmental Advisory Committee, to work with ICANN to expedite the establishment of a global access model that provides law enforcement, intellectual property rights holders, and third parties with timely access to accurate domain name registration information for legitimate purposes. NTIA is encouraged, as appropriate, to require registrars and registries based in the United States to collect and make public accurate domain name registration information.”

Unfortunately, the Internet Corporation for Assigned Names and Numbers (ICANN) has failed to resolve the WHOIS problem. An overwhelming majority of public interest stakeholders have pointed to the failure of ICANN’s WHOIS recommendations, especially the 170+ member Governmental Advisory Committee (“GAC”), including the U.S. representative from the U.S. National Telecommunication & Information Administration (NTIA). The GAC stated:

“ICANN’s Bylaws recognize that WHOIS data is necessary for “the legitimate needs of law enforcement” and for “promoting consumer trust.” The GAC has also repeatedly recognized these important purposes, noting that WHOIS data is used for a number of legitimate activities including: assisting law enforcement authorities in investigations; assisting businesses in combatting fraud and the misuse of intellectual property; safeguarding the interests of the public; and contributing to user confidence in the Internet as a reliable means of information and communication.”

In December 2020, the U.S. National Telecommunication & Information Administration (NTIA) contacted Senate Commerce Committee Chairman Wicker (R-MS) noting:

“[The WHOIS Policy Recommendations failed to address the following basic issues:]

- Measures to ensure data accuracy,
- Policies to allow freely given consent or objection to disclosure of data at the time of domain name registration,
- Rules that distinguish between natural and legal entities and
- Efforts to examine the feasibility of unique contacts to have a uniform anonymized email address.”

In closing, NTIA told Congress that it:

“encourages the Committee to explore alternate approaches to providing federal and local law enforcement, cybersecurity industries, the business and the IP communities—as well as small businesses and the public—prompt and effective access to information they need to build a safe, secure, and trustworthy internet.”
We share the view of the NTIA, many other USG agencies, and global public safety advocates on the importance of restoring WHOIS access. We call on the FTC - through its role as part of the Government Advisory Committee, as well as independently – to work to restore access to WHOIS information to better protect consumers online.

Thank you for your consideration,

Coalition for a Secure & Transparent Internet (CSTI)

The results of this submission may be viewed at:
https://www.ftc.gov/node/1591350/submission/19
Submitted on Monday, January 17, 2022 - 09:41 Submitted by anonymous user: Submitted values are:

First Name: carlos
Last Name: carpi
Affiliation: WBG (on leave) & harvard
Full Email Address: carpi@fas.harvard.edu
Telephone: +16465994801
FTC-Related Topic:
- Consumer Protection
- FTC Operations
Register to speak during meeting: Yes
Link to web video statement:
Submit written comment:
Two Questions:
1. More information on consumer recourse against web platforms, particularly those that involve issues of particularly private nature, such as dating applications. How does the commission see blanket binding arbitration clauses?
2. The FTC is in charge of setting up the HISA (horse racing). But there is a pending lawsuit against its constitutionality. Could the commission comment on how they see these issues going forward?

The results of this submission may be viewed at:
https://www.ftc.gov/node/1591350/submission/7
Majority of franchisees of 7-11 live under unfair contract that states they are a self contractor, while we cannot even control the store temperature and bare all labor costs and other costs. We got no one that can help us and protect our interest with fur franchisor. Many of franchisees put their life savings and a lot of sweat in the store and had to give it up, because there was no money left for them.

If possible to see if 7eleven will pass AB5 test, forensic audit of the system, especially 2019 contracts.

Many of franchisees are afraid of complaining and losing their humble income and losing life savings. Please see how many gave up their store, since Covid 19 hit.

I will do my best to help and inviting you to be a part of nationwide group on Telegram, to understand the magnitude of our frustration.

Thank you for all the hard work

Naor

The results of this submission may be viewed at:
https://www.ftc.gov/node/1591350/submission/39
Submitted on Friday, January 14, 2022 - 18:37 Submitted by anonymous user: Submitted values are:

First Name: Briar
Last Name: Greenway
Affiliation: Multiple Aggravated identity thefts victim
Full Email Address: nuumoxxx@icloud.com
Confirma Email Address: nuumoxxx@icloud.com
Telephone: +17606125517
FTC-Related Topic:
- Consumer Protection
- FTC Operations
Register to speak during meeting: No
Link to web video statement:
Submit written comment: Do you have any plans to help victims — especially those heavily traumatized — recover and protect themselves? I've lost almost everything. Some have lost everything. And there's no help...from the government or the companies responsible — that allow criminals to use their services to destroy peoples' lives - deny even the possibility that they could be in the dark about new technology (Verizon, Apple) They offer no recompense. No remorse. They hide blind behind their privacy policies (Apple). Using them as reasons to not offer true help. They do nothing to change their methodologies that allow such malice to propagate. What will be done to bring these civilian & corporate criminals to justice? What will be done to stop the ransomware and cybercrimes? It feels like the Wild West of the virtual future has no sheriff to protect the people. What will it take? What "important" persons must fall victim to see change?

The results of this submission may be viewed at:
https://www.ftc.gov/node/1591350/submission/7
Submitted values are:

First Name: heather
Last Name: houser
Affiliation: owner
Full Email Address: hhopenacess111@gmail.com
Telephone: +12066710285
FTC-Related Topic: FTC Operations
Register to speak during meeting: Yes
Link to web video statement: google.com
Submit written comment: just want to introduce myself and see about a more private meeting to discuss some concerns further.

The results of this submission may be viewed at:
https://www.ftc.gov/node/1591350/submission/7
Unfortunately, identity theft—like nearly all types of online crime—has risen dramatically over the past few years. In March 2021, the FBI's Internet Crime Complaint Center released its 2020 Internet Crime Report.2 The report includes information from 791,790 complaints of suspected internet crime—an increase of more than 300,000 complaints from 2019—and reported losses exceeding $4.2 billion. In late November 2021, the FBI released a Public Service Announcement detailing one of the latest identity theft challenges: scamming tools to harvest credentials of brand-name consumers.3 These serious and alarming developments in online crime, including identity theft, have been exacerbated by the current lack of access to WHOIS data—the information concerning the entity or person that registers a particular domain name. This information had been publicly accessible since the earliest days of the internet. WHOIS data not only provides transparency, but also is key to governmental and non-governmental investigations and efforts to combat illegal online activity. In an effort to comply with the European Union’s General Data Protection Regulation (“GDPR”), the Internet Corporation for Assigned Names and Numbers (“ICANN”) has required since May 2018 the redaction of critical elements of WHOIS data in the name of privacy.

No one disputes that privacy is an important and fundamental right that warrants protection. But anonymity is not the same thing as privacy. The ability to operate a domain name anonymously, without publicly accessible WHOIS data, must be balanced against other individual and societal rights, including the right to be protected from illegal behavior and the right of democratic governments to protect the integrity of their institutions and processes.

Before ICANN enacted its policy in May 2018 that essentially caused the WHOIS system to go dark, Europol’s European Cybercrime Centre (“EC3”) Advisory Group warned that “it is imperative that any assessment of new WHOIS implementations consider the overwhelming legitimate purpose of processing WHOIS data for [domain name system] DNS abuse enforcement, Internet security and stability, and global cybersecurity efforts.”4 The EC3 Advisory Group described in great detail how “WHOIS data is an indispensable resource for ensuring the security and stability of the global DNS and protecting against DNS-based cybersecurity threats because of its role in facilitating cybersecurity research, threat detection, analysis, and mitigation.”5

1 COA consists of seven leading copyright industry companies, trade associations and member organizations of copyright owners, all of them deeply engaged in the use of the internet to disseminate creative works. The COA members are Broadcast Music, Inc. (BMI); the Entertainment Software Association (ESA); the Motion Picture Association (MPA); the Recording Industry Association of America (RIAA); NBCUniversal; The Walt Disney Company; and WarnerMedia. COA’s main goal since its founding nearly two decades ago (as the Copyright Coalition on Domain Names) has been to preserve and enhance online transparency and accountability.


3 https://www.ic3.gov/Media/Y2021/PSA211123


5 Ibid.
Despite this informed guidance, since the enactment of ICANN’s policy to redact WHOIS data, law enforcement efforts with respect to online illegal activity—including identity theft—have been hampered and online illegal activity has increased. A survey conducted by the Public Safety Working Group of the Governmental Advisory Committee (“GAC”) to ICANN of over 50 law enforcement agencies from around the world detailed how the lack of availability of WHOIS data since ICANN’s adoption of its May 2018 policy has interfered with the work of such government agencies. Prior to the adoption of the ICANN policy in May 2018, only 2% of the law enforcement agencies reported that WHOIS data did not meet investigative needs. Following implementation of the policy, 67% of the agencies reported that WHOIS data did not meet investigative needs.6 We note that the Co-Chair at that time of the GAC Public Safety Working Group was Laureen Kapin, a dedicated and effective FTC public employee.

According to a recent survey of nearly 300 cybersecurity investigators set forth in a report published in June 2021 by the Messaging Malware Mobile Anti-Abuse Working Group and the Anti-Phishing Working Group, the situation has not improved over the past 3 years. The report concludes:

- “94% of our respondents report that redaction of WHOIS data impairs their ability to investigate relationships between malicious domains and actors.”
- “Two-thirds of our respondents indicate that their ability to detect malicious domains has decreased.”
- “The solutions currently discussed at ICANN would not meet the needs of law enforcement and cybersecurity actors in terms of timelines.”
- “Changes to WHOIS access following ICANN’s implementation of the EU GDPR . . . continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyberattacks.”7 We therefore urge that the FTC work closely with the U.S. Congress to consider alternatives outside of ICANN—including U.S. legislation—to restore access to WHOIS data in order to reduce online crimes of all kinds, including identity theft, and to increase public welfare and safety.

Thank you for your consideration of this comment.

6 https://gac.icann.org/presentations/public/icann63%20pswg.pdf
7 https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

The results of this submission may be viewed at:
https://www.ftc.gov/node/1591350/submission/23
Submitted on Tuesday, January 18, 2022 - 19:44 Submitted by anonymous user: 
Submitted values are:

First Name: Kahari
Last Name: Nash
Affiliation: Franchisee Advocate

Full Email Address: Kahari_Nash@yahoo.com
Telephone: +18329019483

FTC-Related Topic: Consumer Protection
Register to speak during meeting: Yes
Link to web video statement:
Submit written comment: It time for the Franchisees to have equal rights under the franchise agreements.

The results of this submission may be viewed at: https://www.ftc.gov/node/1591350/submission/31
From: Federal Trade Commission via Federal Trade Commission <noreply@web1.ftc.gov>
Sent: Tuesday, January 18, 2022 7:45 PM
To: OpenMeeting <openmeetings@ftc.gov>
Subject: Form submission from: Speaker Registration and Public Comment Submission Form for January 20, 2022 Open Commission Meeting

Submitted on Tuesday, January 18, 2022 - 19:44 Submitted by anonymous user: Anonymous Submitted values are:

First Name: Tarlochan
Last Name: Rangi
Affiliation: 7-11
Full Email Address: [REDACTED]
Confirm Email Address: [REDACTED]
Telephone: [REDACTED]
FTC-Related Topic: Consumer Protection
Registered to speak during meeting: Yes
Link to web video statement:
Submit written comment: I am franchisees need to speak

The results of this submission may be viewed at:
https://www.ftc.gov/node/1591350/submission/35
First Name: Noble
Last Name: Shih
Affiliation: 7-eleven franchisee
Full Email Address: nobleut81@aol.com
Confirm Email Address: nobleut81@aol.com
Telephone: +13214435379
FTC-Related Topic: Consumer Protection
Register to speak during meeting: No
Link to web video statement: 
Submit written comment: Look into seven eleven operations through the years. They sell a false dream, no transparency, no credibility when they cannot uphold their end of the franchise agreement. Many franchise owners are suffering and or afraid to speak up in fear of retaliation from the parent company. They are also such a big company they need to be regulated and broken up Tao they do not become a monopoly.

The results of this submission may be viewed at:
https://www.ftc.gov/node/1591350/submission/47
Back to the ongoing mounting damages and the theft, tech-jacked, anti trust, anti competitive, unethical, criminal actions against OUR (if anyone will confirm that) or my intellectual property and protected utility patent. US patent 10885096. What else can I do?

I will say this again. What is worse, knowing someone is in need of help and they are pleading to you for it, or just hurting someone?

Silence is worse. Because Hope remains in the individual asking for the help, as they do everything they can to help themselves they are also wasting valuable time Hoping, waiting to hear back, that is time that they could be searching in other places for help….

Am I even talking to the right people? At least tell me that?

I just read this and wanted to throw up…we had this!

CORONAVIRUS
Wahensky faces CDC burnout as pandemic enters third year

“I feel like one of the most important tools of public health is communication with the public and explaining the why,” said Celine Gounder, an infectious disease specialist who advised the Biden transition’s Covid-19 response. “This isn’t just the CDC … our government is stuck in this very outdated sort of antiquated approach, which is more about public relations than it is about real communication and education.”

——— Forwarded message ————
From: Jon Wickizer
Date: On Tue, Jan 11, 2022 at 1:25 PM
Subject: Fwd: Chairwoman of the Subcommittee on Competition Policy, Antitrust, and Consumer Rights Amy Klobuchar and Director of the Consumer Finance Protection Bureau, Rohit Chopra and in reference to: Impersonation ANPR; FTC File No. R207000 - Antitrust, impersonation fraud, and corruption
To: OpenMeeting, jkhan@ftc.gov, Senator Amy Klobuchar [email redacted]
Cc: Chairwoman of the Subcommittee on Competition Policy, Antitrust, and Consumer Rights Amy Klobuchar and Director of the Consumer Finance Protection Bureau, Rohit Chopra and in reference to: Impersonation ANPR; FTC File No. R207000 - Antitrust, impersonation fraud, and corruption To all that can help,

I have provided various documents, videos and emails, witness names and contacts.
In the past my “pitches” have been for investment purposes. All in efforts to continue to grow the idea and distribute it globally for everyone.

I have always maintained free use for research and the good of humanity.

You can confirm this through my CDC/NIOSH contacts, various presentations, and Pitches.

Now it is much more important for everyone and so it is now a pleading to you....

We had started to collect data and feedback with a focus on helping people.

Giving people control, security and choice. Once my property was stolen, my patent stolen, my efforts to help people in the events of emergencies.

The data that was collected for the CDC, NIOSH and the world. Intellectual property belonging to me as well as researchers within our government. As well as reporting of this criminal action at every local and state level that I trust, to include the FBI. My intention has always been to create something to help people and to hopefully give it to the world. Now I am pitching another sort of request to you for help in this anti-trust, anti-competitive, criminal, civil and publicly corruption situation. A plea for help.

1 September “Problem”

https://youtu.be/zv32jSSCluA

2 October “Solution”

https://youtu.be/bGm97ZVdM

3 November “Barrier”

https://youtu.be/k0jqg2ZIja8

Please, inform me of what I am doing wrong? Perhaps you could give me guidance and direction on what to do right?

Jon Wickizer

Sent from ProtonMail for iOS

The results of this submission may be viewed at:

https://www.ftc.gov/node/1591350/submission/3
First Name: Jon
Last Name: Wickizer
Affiliation: Average person with an idea
Full Email Address: jonwickizer@protonmail.com
Telephone: +13853680768

FTC-Related Topic:
- Competition
- Consumer Protection
- FTC Operations

Register to speak during meeting: No

Link to web video statement: https://vimeo.com/666838424
Submit written comment: Following up for an answer, thank you.

The results of this submission may be viewed at:
https://www.ftc.gov/node/1591350/submission/11