

U.S. House of Representatives
Committee on Energy & Commerce
Subcommittee on Consumer Protection & Commerce

**Hybrid Hearing on:
“Holding Big Tech Accountable: Legislation to Build a Safer Internet”**

Prepared Testimony of Rick Lane
Founder & CEO of Iggy Ventures, LLC
and Child Safety Advocate

Dec. 9, 2021

Chair Schakowsky, Ranking Member Bilirakis, Chairman Pallone, Ranking Member McMorris Rodgers, and Members of the Subcommittee:

Thank you for inviting me to testify. My name is Rick Lane. I am the founder and CEO of strategic advisory firm Iggy Ventures. I also volunteer my time to help child safety organizations combat sex trafficking and other online threats to children. My prior experience includes five years working for House Appropriations Committee Member Rep. Joseph Early (D-MA), five years at a major law firm, two years as director of congressional affairs and e-commerce for the U.S. Chamber of Commerce, and 15 years as SVP for government affairs at 21st Century Fox. Over the past 30-plus years, I had the opportunity to work on almost every major piece of technology-related consumer protection, privacy, and cybersecurity legislation that moved through Congress. I testify today in my personal capacity. My views should not be attributed to any other individual or entity.

Building a more safe, secure, and sustainable Internet will require Congress to focus on four main issues: 1) reforming section 230; 2) creating more transparency in the way Internet platforms operate, while protecting Internet users’ privacy; 3) restoring access to WHOIS data; and 4) updating the Children’s Online Privacy Protection Act (COPPA). These issues do not necessarily need to be address in a single, comprehensive piece of legislation. But they should be *discussed* in a comprehensive fashion. All the pieces must work together. Attachment 1 includes a slide I created in 1998 that illustrates the way technology policy issues interconnect and cut across jurisdictional lines.

We are also running out of time. Web 2.0 was built on top of a Web 1.0 that we now know has cracks in the foundation. And if you believe the latest chatter, we are on the precipice of Web 3.0. Unless we address the Internet’s structural issues, I fear a virtual “metaverse” that occupies even more of our and our children’s lives and collects even more information about us will exponentially exacerbate today’s problems. The status quo works no longer. We need clear rules of the road that promote accountability.

Democrats and Republicans share concerns about the spread of illegal activity online, including identity theft, fraud, illicit sale of opioids, and dissemination of child sexual abuse materials. They share concerns over cybersecurity. And they share concerns over privacy. My hope is that the House and Senate can come together in a bipartisan and bicameral fashion to address those issues, no matter what partisan differences may exist on other issues.

Section 230 Reform

I recognize that section 230 reform is the province of the Communications & Technology Subcommittee and was the focus of a hearing last week. I would be remiss, however, if I didn't take this opportunity to make a few observations on that topic—which concerns the most fundamental form of consumer protection that we have, keeping people safe from harm.

We must return the rule of law to the Internet. I appreciate Congress's decision in 1996 to treat the Internet differently in its nascent years, which I not only supported, but worked to ensure. At this point, however, e-commerce is so ubiquitous as to be just commerce. Until we hold online platforms and other Internet intermediaries such as Cloudflare, Verisign, GoDaddy, the Internet Society, Namecheap, and even the Internet Corporation for Assigned Names and Numbers equally accountable as brick-and-mortar businesses, people will be less safe online.

For that reason, I agree with [Prof. Danielle Citron](#), former House Commerce Committee Counsel [Neil Fried](#), and the [Alliance to Counter Crime Online](#). We need to restore to platforms the ordinary duty of care that would apply but for courts' current, overbroad application of section 230. Congress should amend section 230 to require that platforms and other Internet intermediaries take reasonable steps to curb illegal conduct online as a condition of receiving the section's protections. I further explain the need to restore the duty of care in an article I recently co-wrote in *Tech Policy Press*, provided in Attachment 2.

I am heartened to see how much effort this Committee is putting into reforming section 230. Unfortunately, none of the bills the Communications & Technology Subcommittee considered last week would restore the duty of care, as a recent letter to the Subcommittee from [Victims of Illicit Drugs](#) points out. VOID represents parents who have tragically lost children to the illegal sale of drugs over social media. "These children were not killed by misinformation, bias, hate speech, or algorithms," the letter explains. "They were killed, in part, because platforms negligently, recklessly, or knowingly facilitated illegal activity: in this case, an unlawful drug sale."

Social media such as [Facebook](#), [Instagram](#), [YouTube](#), [Twitter](#), [Snapchat](#), and [TikTok](#) are rife with offers to sell illegal drugs. Although algorithms can exacerbate the problem, transactions often occur without amplification and posts peddling illicit substances are easy to find. Some platforms have taken [helpful steps](#) to address this issue, but other platform operators frequently have their heads in the sand. A former CEO of TikTok, for example, stated at a 2020 Technology Policy Institute event that he had never been told of illicit drug transactions on the platform and [doubted their existence](#). That was a surprising statement since many others knew, including the drug dealers that were using TikTok's [platform](#). Researcher Eric Feinberg and Professor Tim Mackey have over the years [documented such illegal drug sales](#).

If platforms could be held civilly liable for irresponsibly enabling such transactions, they'd be much more likely to pay attention and curb the activity. By making simple language changes to section 230 that restore the duty of reasonable care, Congress could help combat not just Internet opioid sales but all current and future illegal activity online. And in a non-regulatory, pro-free market way that both conservatives and liberals should be able to support: creating meaningful incentives for platforms to find the most effective and efficient ways to prevent online harm.

TikTok could also increase the threat of espionage and cyberattacks in light of the [influence the Chinese government has](#) over both it and ByteDance, the Chinese company that owns TikTok. Indeed, we are confronted with a social networking site that is: a) susceptible to manipulation by a Communist regime with a record of human rights violations; b) growing more rapidly than any U.S. competitor; and c) collecting massive amounts of data on our youngest and most easily influenced demographic in an arms race to develop more sophisticated artificial intelligence. Moreover, TikTok has been proven to have [security flaws](#), as well as agreed to pay a record-setting [\\$5.7 million in 2019 to settle FTC allegations](#) that it illegally collected personal information from children.

Yet section 230 limits TikTok's liability for any nefarious activity by the Chinese government or other third party that the platform might enable. Combining the interests underlying TikTok's surveillance-based business model with the interests underlying China's surveillance-based and oppressive governance model creates an even more dangerous threat in an online world that lacks basic accountability. I include in Attachment 3 an article I wrote addressing the unique problems presented by TikTok.

Transparency

Online platforms and their defenders often [hide](#) behind the First Amendment, arguing that section 230 reform proposals will violate constitutional protections for free expression. Although the First Amendment protects platforms' editorial discretion over "awful but lawful" *content*, that protection does not extend to non-expressive and unlawful *conduct*. That is true as applied to the conduct of the platforms' users as well as the conduct of the platforms themselves in negligently managing such user behavior.

The section 230 reform proposal I recommend above focuses on conduct and so does not run afoul of the First Amendment. In fact, by producing a safer, more lawful online space, it advances core First Amendment interests. Limiting harassment and abuse that can silence different perspectives and communities will increase participation, enhancing transparency and information available to all.

One way, however, to address misinformation, bias, hate speech, or other concerns that would promote free expression rather than hamper it would be for Congress to enact transparency requirements. Indeed, Democrats and Republicans alike have expressed frustration with the opaque and inconsistent way platforms engage in content moderation.

[The Supreme Court has held](#) that the First Amendment allows the government to require that commercial enterprises provide "purely factual and uncontroversial information about the terms under which [their] services will be available," where the "disclosure requirements are reasonably related to the State's interest in preventing deception of consumers." Congress could thus adopt transparency provisions that require each platform to: 1) publicly disclose its content moderation policies; 2) create a process by which users can file a complaint with the platform arguing it did not follow its own policies; 3) create a process by which users can appeal a platform's decision to take down or leave up specific content, or to terminate or not terminate service to a user; and 4) publicly disclose information about the decisions the platform has made to take down or leave up certain content, or to terminate or not terminate service to a user.

Platforms that violate these transparency requirements or their own policies would lose the section 230 shield and might be culpable for breach of contract or a deceptive trade practice. These transparency requirements would also better enable individuals and businesses to decide what platforms to use—potentially prompting new entrants and existing providers to compete based on content moderation practices, thereby promoting innovation. In addition, the public disclosure requirements would allow policymakers, law enforcement, and researchers to track problematic trends—either with users’ online misbehavior or the platforms’ moderation practices—and develop strategies to address them.

WHOIS and Know Your Customer

WHOIS Access

The availability of accurate WHOIS data—which contains basic contact details for holders of Internet domain names—is also critically important and was core to the creation of the [Internet Corporation for Assigned Names and Numbers \(ICANN\)](#). WHOIS data has been public since the founding of the commercial Internet and forms the basis of online transparency, security, and accountability. Access to that information is necessary to protect consumer privacy, promote lawful commerce, and ensure public safety. Indeed, a [DOJ cyber report](#) states that “[t]he first step in online reconnaissance often involves use of the Internet Corporation for Assigned Names and Numbers’ WHOIS database.”

Domain name providers (registries and registrars) often fail to verify WHOIS information from registrants, however, and in 2018 providers increasingly began restricting access to WHOIS data based on an overapplication of the European Union’s General Data Protection Regulation. This is [hindering efforts](#) by cybersecurity firms, public interest groups, the private sector, federal agencies, and law enforcement authorities to protect consumers online by stopping abuses like identity theft, fraud, illegal sale of opioids, human trafficking, state-sponsored espionage, and terrorism.

A 2018 [survey of 55 global law enforcement agencies](#) by the ICANN Public Safety Working Group, for example, revealed that 98 percent found the WHOIS system aided their investigative needs before domain name providers took these unnecessary restrictive measures, as compared to 33 percent after. More recently, a 2021 [survey by the two leading cybersecurity working groups](#) found that restricted access to WHOIS data is impeding investigations of cyberattacks. Two-thirds of the 277 respondents said that their ability to detect malicious domains has decreased, 70 percent indicated that they can no longer address threats in a timely manner, and more than 80 percent reported that the time it takes to address abuse has increased, which means that cyberattacks—and harm to victims—last longer. As the working groups explain:

[C]hanges 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.

* * *

Criminals regularly register large numbers of domains in bulk, often in batches of hundreds or thousands of names at the same time. ... To fight crime and abuse, large datasets are

particularly powerful. ... For this data-driven approach to work, however, high-volume, real-time access to WHOIS records is essentially required. Wait times, rate limiting, inconsistent responses, redacted data ... all decrease response times and data quality.

* * *

Many users in law enforcement, public safety, and cybersecurity of the WHOIS [data] require timely and predictable access to accurate records. This is not only true for those attributing attacks but also for parties relying on bulk data analysis to map cybercriminal infrastructures and detect patterns of abuse. *The survey responses corroborate or are consistent with other studies that have concluded that the changes to WHOIS have undermined cybersecurity and impeded cyber investigations generally* (emphasis added).

The Department of Homeland Security has similarly identified the lack of access to WHOIS data as a significant and growing problem. The DHS stated in a July 16, 2020, letter to Rep. Bob Latta, then chairman of the House Commerce Committee’s Consumer Protection Subcommittee, that if the agency “had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain.”¹ The FTC and FDA have also expressed concern.²

The Department of Commerce has been outspoken about the United States’ [concern over the removal of public access](#) to accurate WHOIS information. The Department sent a letter as far back as April 4, 2019, directing ICANN “to deliberately and *swiftly* create a system that allows for third parties with legitimate interests, like law enforcement, IP rights holders, and cybersecurity researchers to access non-public data critical to fulfilling their missions.”³ The letter observed that “[w]ithout clear and meaningful progress, alternative solutions such as calls for domestic legislation will only intensify and be considered.”⁴

Yet after almost five years, ICANN has failed to solve the problem. The time has therefore come for this Committee to pass legislation requiring domain name providers to once again make WHOIS information available for legitimate purposes. Such legislation would help solve cyber issues at zero cost to taxpayers. Even the European Union’s proposed [2.0 version of its Directive on Security of Network and Information Systems](#) included language to address the problem of a “dark” and inaccurate WHOIS. I have included in Attachment 4 an article I wrote discussing how

¹Letter from Raymond Kovacic, Assistant Director, Office of Congressional Relations, DHS, to Rep. Bob Latta (July 16, 2020).

²See Letter from Joseph Simons, FTC Chairman, to Rep. Bob Latta (July 30, 2020) (expressing concern over new domain name provider policies “that significantly limit the publicly available contact information relating to domain name registrants” and stating that “[t]he FTC would benefit from greater and swifter access to domain name registration data.”); Letter from Karas Gross, Associate Commissioner for Legislative Affairs, FDA, to Rep. Bob Latta (Aug. 13, 2020) (stating that “[a]ccess to WHOIS information has been a critical aspect of FDA’s mission to protect public health” and that the reduced availability of WHOIS data “has had a detrimental impact on FDA’s ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients.”).

³Letter from David J. Redl, Assistant Secretary of Commerce for Communications and Information, to Cherie Chalaby, Chair, ICANN Board of Directors (April 4, 2019).

⁴*Id.*

the lack of WHOIS access is hindering anti-espionage and anti-terrorism efforts, and in Attachment 5 a letter from the Coalition for Online Accountability discussing the pressing need to solve the WHOIS problem. Congress and the Department of Commerce can no longer continue to put ICANN’s multistakeholder process over the health, safety, and cyber security of the American people.

Know Your Customer Requirements

Online intermediaries other than domain name providers also have a role to play. The failure of many intermediaries to verify their customers’ identities aggravates today’s growing epidemic of harmful and illegal conduct online in two ways. First, people are more likely to engage in antisocial and unlawful conduct if they believe their identities are hidden. Second, holding individuals and entities accountable becomes harder if no one knows who they are.

That is why I helped submit comments on behalf of [thirteen online safety organizations](#) asking the Department of Commerce to adopt Know Your Customer-type obligations for Internet intermediaries as the Department implements Executive Order No. 13984 on “Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities.” People often have good reasons for protecting their identities, such as securing their safety from those who would cause them harm and avoiding retribution for whistleblowing. Verifying identities for use of Internet services can occur, however, while maintaining safeguards that prevent disclosure except in appropriate circumstances.

FinTech Child Privacy Protection Gap

No area of consumer protection is more important than establishing responsible policies to protect children in the marketplace. Yet while platforms and other Internet intermediaries have made it more difficult to deter or track individuals engaged in unlawful activity online, they have been even less steadfast in [protecting our children](#).

This is especially true in the area of online privacy and market dominant digital payment apps that target children and collect and exploit “[a shocking amount of](#)” their data. That data can potentially lay the foundation for profiling and [targeting child victims](#) or identity theft and fraud that can undermine a child’s financial future – especially if a company is hacked or breached and this information ends up in dark web data trading markets.

The Children’s Online Privacy Protection Act, enacted in 1998, makes it unlawful for a “website or online service” to collect personal information from a child under thirteen—whether for the service’s own use or to sell to others—without first obtaining parental consent.⁵ This is essentially an opt in. By contrast, the Gramm-Leach-Bliley Act, enacted in 1999, makes it unlawful for a “financial institution” to disclose to a non-affiliated third party (but not to use itself) any non-public personal information about someone without offering them an opportunity to opt-out.⁶ That space between ages 12 and 18 is the FinTech Child Privacy Protection (FTCPP) gap where young

⁵See Omnibus Consolidated Appropriations, Pub. L. No. 105-277, div. C, tit. XIII, 112 Stat. 2681, at 728-35 (1998) (codified at 15 U.S.C. §§ 6501-06).

⁶See Pub. L. No. 106-102, tit. V, 113 Stat. 1338, 1436-45 (1999) (codified at 15 U.S.C. §§ 6801-09).

consumers are not adequately protected but existing law does not empower parents to give them meaningful oversight and support.

This FTCPP gap is especially harmful as we move toward a cashless society, however—a trend accelerated by the pandemic. Children today are more frequently engaging in financial transactions with digital wallets, both online and in stores. The parental opt-in requirements of COPPA certainly do not apply to children that use these digital services if they are 13 or older. Indeed, in some cases the FTCPP gap may even reach down to children who are younger than 13 depending on whether the entity doing the collecting qualifies as a financial institution as opposed to a website or online service. Unfortunately, some operators of financial applications may be exploiting this gap to use or sell the data of the kids they are currently courting to their services, [as *Vice* reported earlier this year](#). That also means data on children is becoming more susceptible to data breaches.

The good news is that at least one FinTech provider is going above and beyond the legal requirements. [Rego Payment Architectures](#)—a company I provide strategic advice to and in which I am an investor—has incorporated COPPA privacy by design into its [Mazoola](#) financial application and pay button, producing the only COPPA certified digital payment app on the market. Mazoola allows parents to create digital accounts for their children but collects no personally identifiable information about the kids. All Mazoola knows is that the account is attributable to the parents and even there the company collects the bare minimum needed to comply with existing Know-Your-Customer and banking laws. The parents can then set chores or other tasks, pay allowances, set limits on the amount of money the kids may spend and where, and even reject specific purchase attempts in real time.

Rego is doing all this voluntarily. Which raises another point. The House and Senate Judiciary Committees' antitrust efforts may inadvertently harm such voluntary efforts by forcing technology companies to [open their platforms](#). Without taking a position on the need for new antitrust legislation or the competitive impact of closed systems, it is true that closed systems are easier to keep safe. I do believe this Committee should keep an eye on the antitrust debates to make sure legislative efforts there do not make your job here harder. I have similar concerns about the impact of end-to-end encryption on the ability to keep children safe, absent creation of a lawful mechanism to access information for legitimate purposes. In this area, we should be wary of unintended consequences.

Thank you again for giving me the opportunity to participate today. I look forward to your questions and to continue working with you on these issues. We all must work together to fix these problems because, at the end of the day, it is the right thing to do.

Broadband

- High Speed Data & Video Services -

Encryption/DRM

- Data Scrambling Technology -

Digital Signatures

- Authenticating Electronic Commerce Transactions -

Online Privacy/Profiling

- Using Personal Information -

Domain Names

- ICANN -

Local/State Governments

Administration

Private Sector

Network Security

- Hacking/Cyberterrorism -

Trade Laws

- World Trade Organization -

Internet Taxation/Tariffs

- Tax Treatment of E-commerce -

Digital Copyright

- Copyright Protection for Digital Works -

Database Protection

- Electronic Collections of Data -

International

Congress

Judiciary

Mail Marketing

- Spamming -

ABOUT

CONTRIBUTORS

NEW VOICES

NEWSLETTER

PODCAST

DONATE



TECHNOLOGY, POWER, POLICY AND PEOPLE

Section 230 Reform Naysayers Ignore Clear Problems Online-and the Clear Solutions

PUBLISHED OCTOBER 13, 2021



Skeptics of reforming Section 230 of the Communications Act, which limits platform liability, routinely diminish the unlawful and harmful conduct that online platforms facilitate through their own irresponsible behavior, as well as constitutional proposals that can help address this problem.

Take, for example, Jeff Kosseff and Daphne Keller's Oct. 9 *Washington Post* [Perspective](#), "Why outlawing harmful social media content would face an uphill legal battle." In it, the authors focus on the "misinformation, toxicity, and violent content" that social media amplify. They point out that algorithmic amplification of awful but lawful speech is protected by the First Amendment, making many proposed legislative responses potentially unconstitutional.

This sidesteps, however, not only the platform carelessness highlighted in the recent series of four Senate hearings on [protecting consumers and kids](#), but also the constitutional approach that [Professor Danielle Citron](#) and [we](#) have [each](#) put [forward](#) to address it: amending Section 230 so that platforms cannot invoke the liability shield unless they take reasonable steps to curb *unlawful conduct* on their services.

Ordinarily, businesses have a [duty of care](#) to protect one customer from harming another customer or the public. A hotel can be held civilly liable if it doesn't do enough to limit prostitution on its premises. A nightclub can be held civilly liable if it doesn't do enough to limit drug trafficking on its dance floor. A pawn shop can be held civilly liable if it doesn't do enough to limit fencing in its store.

These and many other situations have analogs in the online world. But a 1997 court interpretation of Section 230 granting platforms overbroad immunity for their irresponsible behavior has had the effect of preventing application of the duty of reasonable care in such situations. That decision further enables the platforms' "move fast and break things" culture, to borrow a phrase from Mark Zuckerberg.

As more of our social, economic, and political lives have moved online, this dereliction of the rule of law makes the public less safe and removes judicial recourse. Adding insult to injury, it gives online platforms an inappropriate competitive advantage over their brick-and-mortar rivals, which rightfully must expend resources to ensure their own behavior does not facilitate illegal or harmful activity.

Restoring the duty of care for online platforms, as we suggest, does not require repeal of Section 230. Nor does it involve government restriction of lawful speech. It simply gives victims access to the courthouse steps when a platform irresponsibly facilitates *unlawful or harmful conduct*. The victims still must prove their cases, but at least they can be heard.

The reasonableness standard has been developed over more than 100 years of judicial precedent that courts, victims, and platforms can rely on. It provides a mechanism that can account for platform size and the amount of harm, so that smaller platforms and startups are not treated as if they are Facebook or YouTube. And it can adjust as online problems and potential solutions evolve. If the platforms and their

defenders are worried about abusive litigation, they should join the tort reform movement, not defend a distortive, harmful, and unjust carve-out for social media.

There is also a constitutional way to address awful but lawful misinformation, toxicity, and violent content on social media—as well as platforms' erratic and opaque content moderation practices: transparency requirements.

Congress cannot require or prohibit platforms to take down or leave up lawful speech. The First Amendment leaves those decisions to the platforms' discretion.

But the Supreme Court has held that the First Amendment *does* allow the government to require that commercial enterprises provide “purely factual and uncontroversial information about the terms under which [their] services will be available,” where the “disclosure requirements are reasonably related to the State's interest in preventing deception of consumers.”

Congress could adopt transparency requirements that require platforms to: 1) publicly disclose their content moderation policies; 2) create a process by which users can file a complaint with the platform arguing it did not follow its own policies; 3) create a process by which users can appeal a platform's decision to take down or leave up specific content, or to terminate or not terminate service to a user; and 4) publicly disclose, subject to certain privacy protections, information about the decisions the

platform has made to take down or leave up certain content, or to terminate or not terminate service to a user.

Platforms that violate these transparency requirements or their own policies would lose the Section 230 shield and might be culpable for breach of contract or a deceptive trade practice. That would give users a venue when the platforms moderate in an inconsistent way.

These transparency requirements would also better enable individuals and businesses to decide what platforms to use—potentially prompting new entrants and existing providers to compete based on content moderation practices, promoting innovation.

In addition, the public disclosure requirements would allow policymakers, law enforcement, and researchers to track problematic trends—either with users' online misbehavior or the platforms' moderation practices—and develop strategies to address them.

Focusing on platforms' careless facilitation of unlawful or harmful conduct, along with these two constitutional approaches, would allow Congress to advance a freer, safer, more transparent internet. The platforms shift focus to lawful but awful speech because that problem is harder to solve. Entertaining that misdirection only benefits tech firms, the central beneficiaries of the status quo.

Neil Fried

Neil Fried launched DigitalFrontiers Advocacy in January 2020, bringing more than 25 years of experience in the public and private sectors, and testified before Congress on section 230 reform in June of that year. From 2013 to 2020, Neil was senior vice president for congressional and regulatory affairs at the Motion Picture Association. He joined the MPA in 2013 from the House Energy & Commerce Committee, where he served as counsel and ultimately chief counsel on media and technology law issues for close to 10 years. Prior to working on the Hill, Neil represented clients before Congress and the Federal Communications Commission while at the D.C. offices of two law firms: Verner, Liipfert, Bernhard, McPherson and Hand; and Paul Hastings. He helped implement the 1996 Telecommunications Act as an attorney with the FCC from 1996 to 2000. Before coming to the FCC, he was a John S. and James L. Knight Foundation law fellow at the Reporters Committee for Freedom of the Press.

Rick Lane

Rick Lane is a tech policy expert, child safety advocate, and the founder and CEO of Iggy Ventures. Iggy advises and invests in companies and projects that can have a positive social impact. Prior to starting Iggy, Rick was the Senior Vice President of Government Affairs of 21st Century Fox/News Corporation. Rick was responsible for coordinating the development and implementation of the Company's public policy activities. Before joining 21st Century Fox, Rick was the first Director of Congressional Affairs focusing on E-Commerce and Internet public policy issues for the United States Chamber of Commerce. Prior to working at the Chamber, Rick was employed by the international law firm of Weil, Gotshal & Manges LLP (WG&M) as the Director of Legislative Affairs. While at Weil, he advised and represented clients before Congress on a variety of legislative matters affecting the technology and telecommunications industries. From 1988 to 1993, he worked as an Associate Staff member to the House Appropriations Committee. His primary responsibilities involved technology, telecommunications, tax, education, labor and related issues.

Gretchen Peters

Gretchen Peters is Executive Director of the Alliance to Counter Crime Online. She conducts complex research and investigations of organized crime and corruption.

The Trichordist

Artists For An Ethical and Sustainable Internet #StopArtistExploitation

Tag: Tik Tok Drug Dealers

Crouching Tiger, Hidden Dragon: Broad and Antiquated CDA 230 Immunity for TikTok Could Aid China's Secret Efforts to Undermine U.S. Cyber-Security: Guest Post by Rick Lane

I believe there are only two public policy issues that President Trump and Vice President Biden agree upon: The status quo of Section 230 of the 1996 Telecommunication Act is no longer acceptable; TikTok is a threat to our cyber and national security.

Interesting enough, these two issues are interlinked. Section 230 of the Communications Decency Act (CDA 230) gives free reign to Internet platforms operating in the United States to act with impunity as it relates to user generated content. Predictably, this has led to unintended and destructive consequences. But, left unsaid is what Big Tech doesn't want anybody to realize – CDA 230 also unwittingly shields China as America's top geopolitical adversary challenges U.S. national and economic security right here at home.

According to Bloomberg, Chinese-controlled "ByteDance/TikTok, led by Zhang Yiming, is becoming a viable rival to the dominant American online behemoths, Facebook Inc. and Alphabet Inc.." Last year, TikTok's net profit was approximately \$3 billion and the company estimates that it has about 80 million monthly active users in the United States, 60% of whom are female and 80% fall between the ages of 16 and 34. Of particular concern is that 60% of TikTok users are Gen Z, which is the largest generational cohort in American history and will include 74 million people next year.

As a champion of free markets, I would normally be among the first to applaud an upstart bringing a competitive “A” game to challenge dominant incumbent players no matter where they are based. But we have learned from experience that homegrown social networking companies like Facebook/Instagram, Google, and Twitter exert dominant and controversial influence in U.S. public policy debates – what sort of foreign influence should we expect TikTok to exert on this year’s election.

Lately, I’ve found myself asking should I really be concerned?

A recent article by Larry Magid was the tipping point for me in this debate. The headline of the article was, “How A 51-Year-Old Grandmother and Thousands of Teens Used TikTok to Derail A Trump Rally & Maybe Save Lives.” Magid lays out the series of events illustrating how attendance at a Trump rally was manipulated by a viral video of a grandmother from Iowa. It sounds innocent enough until you realize that the inflated numbers of expected attendees started when fans of K-pop, the popular Korean music genre, ordered free rally tickets from the Trump campaign with no intention of actually attending. Next, according to the article, the “grandmother from Iowa” posted a video on TikTok urging her mostly young viewers to “Google two phrases, ‘Juneteenth’ and ‘Black Wall Street,’” before also suggesting that they register for two free tickets to the Trump rally. Her video post went viral and motivated young TikTok users to request hundreds of thousands of tickets.

After reading this, I was left with a simple question: Whether Trump or Biden, doesn’t it bother anyone else that a Chinese-controlled social network was used to interfere with an American presidential campaign event at the same time that tensions between our two countries are escalating? Even Vice President Biden has banned TikTok from campaign phones and computers. As Mr. Magid’s article acknowledges, “(i)t’s long been known that social media can have a huge impact on politics. That’s why Russia tasked a state-run agency to flood social media with posts and ads to get Donald Trump elected.”

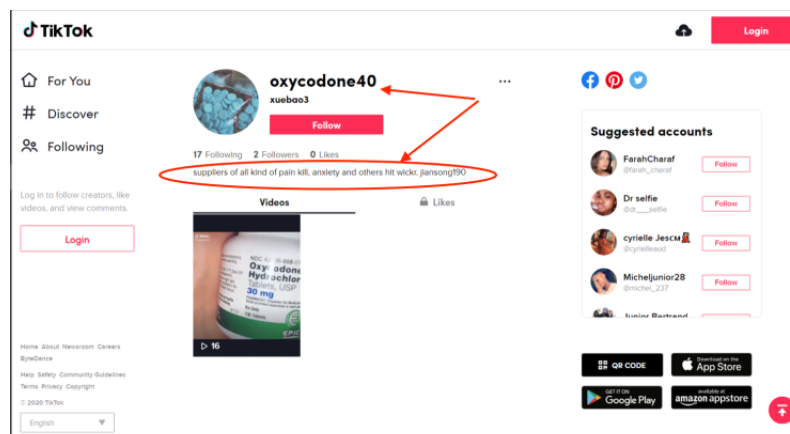
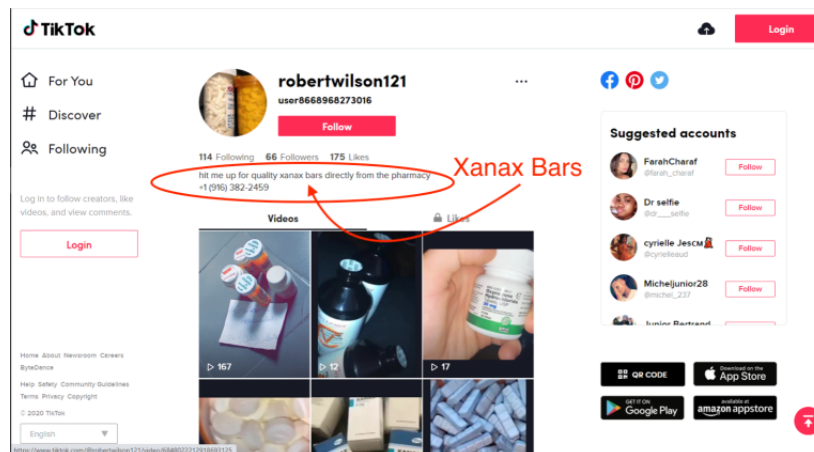
Two additional facts build on the story told by Magid. Another recent article, titled “Anonymous Hackers Target TikTok: ‘Delete This Chinese Spyware Now,’” states that TikTok is “a data collection service that is thinly veiled as a social network. If there is an API to get information on you, your contacts, or your device, they’re using it.” The other fact to connect is that the key driver for algorithms and artificial intelligence, especially when dealing with human behavior, is vast data on human interaction. It is one of the main reasons that Microsoft is so interested in buying TikTok.

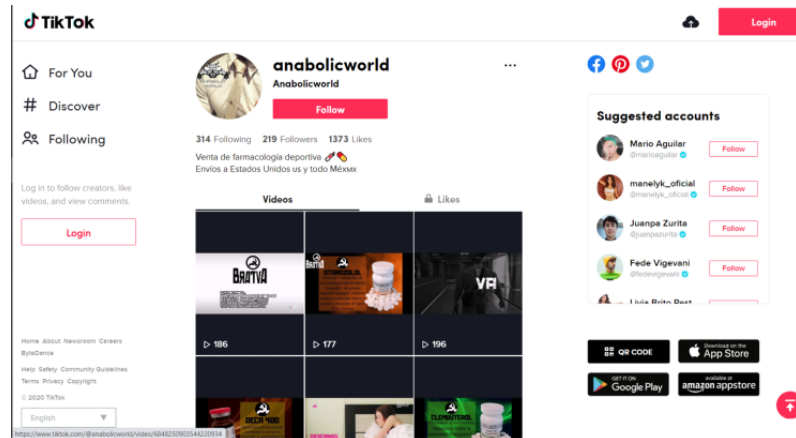
So now we are confronted with a Chinese based “social networking” site growing more rapidly than any homegrown US competitor and collecting more data on our youngest and most easily influenced demographic at the same time that China, Russia, and Iran are using social networks to undermine our democracy. Let’s not forget that this social networking site has been proven not to be secure and agreed to pay \$5.7 million to settle Federal Trade Commission (FTC) allegations that it illegally collected personal information from children, the largest civil penalty ever obtained by the FTC in a children’s privacy case.

But most alarming is that TikTok is protected by CDA 230 and cannot be held accountable for the actions of its “users” even if those “users” happen to be foreign governments. For example, if the Chinese government is leveraging TikTok for its own strategic advantage, the US government has no recourse against TikTok for these activities. The impunity provided by CDA 230 to TikTok, as well as Chinese and other hostile governments, directly threatens our democratic process. Even more troubling is the fact that TikTok, along with Facebook and other social networking sites, cannot be held responsible for illegal conduct occurring on their platforms – even when they know about it.

Besides the potential of interfering with our elections, TikTok also continues to facilitate the sale of illegal drugs. Below are three screenshots of illicit activity being perpetrated on TikTok. The first two images show illegal drug sales of opioids and the other shows illegal drug sales of steroids. Remember, TikTok’s core demographic and the intended audience for these posts consists primarily of members of Gen Z, those born between 1995 and 2012 –our children. [Similar to Google’s near-indictment and \$500,000,000 fine for violating the Controlled Substances Act (<https://musictechpolicy.files.wordpress.com/2010/09/google-agreement.pdf>).]

(Screenshots Provided by Eric Feinberg)





I will leave you with a quote from [a recent speech](https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states) (https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states) at the Hudson Institute by FBI Director Christopher Wray.

He stated:

“The Chinese government is engaged in a broad, diverse campaign of theft and malign influence, and it can execute that campaign with authoritarian efficiency. They’re calculating. They’re persistent. They’re patient. And they’re not subject to the righteous constraints of an open, democratic society or the rule of law... China, as led by the Chinese Communist Party, is going to continue to try to misappropriate our ideas, influence our policymakers, manipulate our public opinion, and steal our data. They will use an all-tools and all-sectors approach—and that demands our own all-tools and all-sectors approach in response.”

For addressing this clear and present danger, the United States must modify CDA 230 and ensure that we have all the tools necessary to hold TikTok accountable for criminal activity that occurs by “others” on their platform. Importantly, this includes illegal actions taken by the Chinese government to misappropriate the site, and the massive amounts of data it collects, in order to inflict harm on the US and its allies. Finally, we must avoid inadvertently making this problem worse by spreading the excessively broad and antiquated immunity of CDA 230 through trade agreements with other countries.

[Rick Lane is the founder and CEO of IGGY Ventures](https://www.worldwithoutexploitation.org/bios/rick-lane) (https://www.worldwithoutexploitation.org/bios/rick-lane). IGGY advises and invests in technology startups and public policy initiatives that can have a positive societal impact. Rick served for 15 years as the Senior Vice President of Government Affairs of 21st Century Fox. Before joining Fox, Rick was the Director of Congressional Affairs focusing on e-Commerce and Internet public policy issues for the United States Chamber of Commerce.

September 20, 2020 by Trichordist Editor

[Blog at WordPress.com.](https://www.wordpress.com)



CONGRESS MUST ACT NOW!

Published on December 22, 2020



Rick Lane
Strategic Advisor

9 articles

✓ Following

On January 10, 2020, the President issued an executive order strengthening the economic sanctions against Iran. While the Iranian government announced that the ballistic missile attacks on Iraqi bases

used by U.S. forces concluded their response to the killing of General Soliemani, increased tensions between the U.S. and Iran are expected to continue and Iran's cyber capabilities will continue to pose a threat to U.S. interests. Director of National Intelligence John Ratcliffe said both Iran and Russia have obtained US voter registration information in an effort to interfere in with the 2020 Presidential election. The Cybersecurity and Infrastructure Security Agency (CISA) recently announced the compromise of U.S. government agencies, critical infrastructure entities, and private sector organizations, most likely by Russia, beginning in at least March 2020. Recognizing those threats, the U.S. must ensure that it has the tools necessary at its disposal to defend itself – including access to WHOIS data.

WHOIS data is the registration information for *who is* behind a particular website. Much like public land and title records that demonstrate ownership of a physical location, WHOIS records had been publicly available since the inception of the Internet. WHOIS records have been used by law enforcement, cyber security experts and consumer advocates to identify malicious websites and either block, isolate or take additional action. Unfortunately, the recent, and overly broad, interpretation of the European Union's General Data Protection Regulation (GDPR) has resulted in this information being redacted and going almost entirely dark. No longer can law enforcement or cyber security firms quickly identify registration information behind a website and link that information to other, potentially harmful website.

Concerns around WHOIS information going dark have been well documented. In a survey of law enforcement agencies from around the world presentation to the Public Safety Working Group at ICANN, 98 percent of respondents indicated that WHOIS information at least partially met their investigative needs prior to implementation of the EU GDPR. Since then, only 8 percent of those same respondents said that WHOIS still meets their investigative needs. At a 2019 briefing on Capitol Hill, Jason Gull, Senior Counsel in the Department of Justice's Computer Crime and Intellectual Property Section said, "We are finding that WHOIS is turning into 'WHO WAS.' We have historical information about WHOIS from a year ago and that information is like having an old phonebook." Other agencies, including the Food & Drug Administration and Drug Enforcement Administration, have also expressed their frustration with this resource going dark.

Russia, Iran, China and its surrogate forces are well-known to be expert cyber-warriors. In a very short period of years, cyber warfare has gone from being an element of science fiction to a grim reality. Because it is highly asymmetric (very few expert hackers can cause widespread effects) and deniable (forensic attribution is not easy) many experts believe that cyber will become a preferred method attack and disruption that countries will use.

That is certainly true of countries like Russia, Iran and China. They have a history of using cyber tools effectively. In fact, several Iranians have been indicted in the U.S. justice system for their roles in cyber

activities targeting America and American entities. In 2018, an investigation by FireEye (using registration data) discovered over 2,800 inauthentic social media accounts originating from Iran that were ultimately removed from social media platforms. These accounts were designed to impersonate U.S. political candidates and influence media campaigns involving Iranian interests.

Dealing with the WHOIS problem is vital, and the urgency to do so is only increasing. Unfortunately, current estimates for regaining access to WHOIS by correcting the interpretation of the GDPR won't be available for three years or more. Now is the time for Congressional leadership. Without WHOIS, our vulnerabilities will continue to persist and investigations into not only cyber-frauds and cyber-warfare, but drug cases, intellectual property cases and other problems will be hurt.

As was stated by the U.S. Department of Homeland Security in a July 16, 2020 letter to Representative Robert Latta, "HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations... Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. If HSI had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain."

Strengthening the cyber resilience of both public and private sector organizations is a matter of national security. We should expect that adversaries will continue to focus efforts to gather intelligence and cause disruptions through cyber-activities. For Congress and the Administration to ignore the WHOIS problem, or wait for the failed ICANN process to fix it, is turning a blind eye to an extremely serious risk to our nation. Congress needs to step in and address this vital weakness in our cyber defenses. Congress needs to enact WHOIS legislation now that will ensure that those who are protecting our national cyber infrastructure have all the tools they need to make America and the world more safe.

Report this

Published by



Rick Lane
 Strategic Advisor
 Published · 11mo

9 articles

✓ Following

[#cybersecurity](#) [#isoc](#) [#contentprotection](#) [#icann](#) [#platformresponsibility](#) [#verisign](#)
[#consumerprotection](#) [#infosec](#) [#privacy](#) [#WHOIS](#) [#ICANN](#) [#GODADDY](#)
[#dataprotection](#)



Like



Comment



Share



4 · 2 comments

Reactions

Attachment 5



Coalition for Online Accountability

November 30, 2021

The Honorable Maria Cantwell
Chairman
The Honorable Roger Wicker
Ranking Member
Senate Committee on Commerce, Science and Transportation
512 Dirksen Senate Building
Washington, D.C. 20510

Re: Nomination of Alan Davidson as Assistant Secretary of Commerce for Communications and Information

Dear Chairman Cantwell and Ranking Member Wicker:

We at the Coalition for Online Accountability (“COA”)¹ have been deeply involved with ICANN related matters including those related to domain registrant information—often referred to as WHOIS data—and abuse in the Domain Name System (“DNS”) for nearly twenty years. In light of the National Telecommunications and Information Administration (“NTIA”)’s letter last year of December 23, 2020² to then Chairman Wicker and the developments at ICANN and the significant growth of cybercrime and DNS abuse since that time, we are writing to request that the information set forth below and the questions posed at the end of this letter be made part of the official record in connection with the hearing on December 1, 2021 to consider Alan Davidson as Assistant Secretary of Commerce for Communications and Information and head of NTIA.

As set forth in President’s May 2021 Executive Order on Improving the Nation’s Cybersecurity *“The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, and ultimately the American people’s security and privacy”* and that *“the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life.”*³

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.

²² <https://secureandtransparent.org/wp-content/uploads/2021/01/NTIA-Senate-Letter-12-23-20.pdf>

³ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

A specific component of this challenge concerns the current lack of access to domain name registration data (also called “WHOIS data”)—the information that identifies the organization or individual that owns a website operating under a particular domain name. From the earliest days of the Internet until May 2018, WHOIS data was publicly accessible and used for investigating and mitigating illegal online activity by both public and private sector organizations, including law enforcement agencies, cybersecurity investigators, network technology professionals, child protection organizations, patient safety organizations, consumer welfare organizations, and anti-counterfeiting and anti-piracy organizations.⁴

Yet since the enactment of policies by the Internet Corporation for Assigned Names and Numbers (“ICANN”) in May 2018 to attempt to comply with the European Union’s General Data Protection Regulation (“GDPR”), the WHOIS system has essentially gone dark. As noted in a recently released study by Interisle, currently “86.5% of registrants cannot be identified via WHOIS.”⁵ Letters have been written by a number of federal agencies describing how the current lack of access to WHOIS data is interfering with their investigations of a broad array of online criminal activity and is increasing risks to public safety and welfare. For example, the Department of Homeland Security set forth a very specific example in a letter last year to Congressman Robert Latta as follows:

“As a recent example of GDPR inhibiting HSI investigations, the HSI Cyber Crime Center (C3) Cyber Crimes Unit identified several websites posing as legitimate coronavirus disease 2019 (COVID-19) fundraising organizations, but are actually fraudulent. These websites claim to be sites for entities such as the World Health Organization, United Nations’ foundations, and other non-governmental organizations, and appear to be legitimate. When HSI conducted WHOIS queries for these domains, most of the subscriber information was redacted as a result of GDPR. Having increased and expedient access to domain name registration information would have allowed HSI to identify the registered owners of the domains expeditiously in order to prevent further victimization by these illegitimate fundraising websites.”⁶

As stated by NTIA in its letter of December 23, 2020 to this Committee, “the importance of this [WHOIS] data cannot be overstated.” Furthermore, we support NTIA’s conclusion that the policy, which has been under development by ICANN’s multi-stakeholder process for now over three years, falls drastically and unacceptably short of meeting the public interest, particularly in the areas of safety, security, consumer welfare and protection of intellectual property. These difficulties and obstacles were further highlighted in a recent report published in June 2021 by the Messaging Malware Mobile Anti-Abuse Working Group (“M3AAWG”) and the Anti-Phishing Working Group (“APWG”).⁷ Based upon a survey of nearly 300 cybersecurity practitioners, the report concluded:

- *“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.” (emphasis added)*

M3AAWG and APWG wrote to the ICANN Board and CEO at the end of September 2021 to inform them of the study and to offer detailed specific suggestions to improve the WHOIS situation in order to reduce cyberattacks and cybercrime.⁸ ICANN responded in November with a terse reply that stated in relevant part, “The ICANN policy development process cannot define, correct ambiguities under, or change international law.”⁹

⁴ Before May 2018, WHOIS data had been a public directory since the early 1980s. For a brief history of WHOIS, see:

<https://whois.icann.org/en/about-whois#field-section-3>

⁵ <http://www.interisle.net/ContactStudy2021.html>

⁶ <https://secureandtransparent.org/wp-content/uploads/2020/09/20-02497-ICEs-Signed-Response-to-Representative-Latta.pdf>

⁷ https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

⁸ <https://www.icann.org/en/system/files/correspondence/cadagin-cassidy-to-marby-et-al-30sep21-en.pdf>

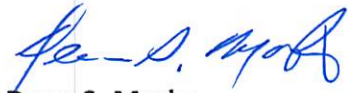
⁹ <https://www.icann.org/en/system/files/correspondence/marby-to-cadagin-cassidy-04nov21-en.pdf>

The 170+ member Governmental Advisory Committee (“GAC”) to ICANN stated in June 2020 with respect to WHOIS data, “[A]ccess to this information is essential to allow public authorities and other relevant entities to serve objectives such as law enforcement, cybersecurity, consumer protection or the protection of intellectual property. Such access remains a high priority for the GAC.”¹⁰ Nevertheless, more than three years following the implementation of ICANN’s policies to redact WHOIS data, access has been overwhelmingly unavailable and ICANN states it cannot do anything further because it cannot define the law.

QUESTION FOR NOMINEE DAVIDSON: Will you, as Assistant Secretary of Commerce and head of NTIA, work with us in Congress on legislative or regulatory measures to address this situation and restore access to WHOIS data? Given that the overwhelming majority of generic top-level domain names are administered by U.S. companies, are you willing to work with us on U.S. legislation that will require that U.S. based domain name registrars and registries: (i) verify the accuracy of the WHOIS data that they collect, and (ii) make such data publicly accessible? Such legislation will not cost the federal government a single dollar and yet it will significantly improve the ability of both government agencies and private sector cybersecurity professionals to investigate, mitigate and prevent cyberattacks and a broad array of cybercrime.

Thank you for your consideration.

Sincerely,



Dean S. Marks

Executive Director and Legal Counsel

Coalition for Online Accountability (“COA”)

E-mail: ed4coa@gmail.com

¹⁰ See ICANN67 GAC Communique at: <https://gac.icann.org/contentMigrated/icann67-gac-communique> at p. 7

4 November 2021

To: Amy Cadagin, Executive Director; Peter Cassidy, Secretary General
Cc: Maarten Botterman and Rod Rasmussen

Dear Ms. Cadagin and Mr. Cassidy,

Thank you for your [letter dated 30 September 2021](#) regarding findings from the M3AAWG and APWG WHOIS Report presented to ICANN in June 2021. We acknowledge receipt of the recommendations contained in the letter. As stated in our 7 July 2021 [response to your 8 June 2021 letter](#), the consensus policy recommendations developed by the ICANN community for a System for Standardized Access/Disclosure (SSAD) extend as far as the community determined possible, due to the ambiguity and legal constraints that exist under the GDPR. The ICANN policy development process cannot define, correct ambiguities under, or change international law.

The ICANN org appreciates M3AAWG and APWG's continued participation and engagement in the multistakeholder model and also noted your active participation in the recently completed [ICANN72 Annual General Meeting](#).

Regards,



Göran Marby
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers (ICANN)