



TIME TO REFORM CDA230

Testimony to the House Subcommittee on Communication and Technology and the Subcommittee on Consumer Protection and Commerce.

Delivered at the 16 October 2019 Hearing entitled, "Fostering a Healthier Internet to Protect Consumers."

Testimony by Gretchen Peters, Executive Director

Alliance to Counter Crime Online, Washington DC



Chairman Doyle, Chair Schakowsky, Ranking Members Latta and McMorris Rodgers and members of the Subcommittees: It's an honor to be here today before you to discuss one of the premier security threats of our time, one that your committees are well-positioned to solve.

I am the executive director of the Alliance to Counter Crime Online.

Our alliance is made up of academics, security experts, NGOs and citizen investigators that have come together to push serious organized crime and terror activity off the Internet.

Under the original intent of CDA Section 230, there was to be a shared responsibility between tech platforms, law enforcement, and organizations like ACCO.

However, tech firms are failing to uphold their end of the bargain and, because of overly broad interpretations by the courts, tech firms now use CDA 230 as a shield instead of a sword.

Congress must modify CDA 230 and create legal and financial incentives to hold tech firms accountable when they are knowingly or negligently facilitating illegal activity.

I want to thank you for your interest in our research and for asking me to join the panel of witnesses testifying today. Like you, I had hoped to hear the testimony of U.S. Trade Representative, because keeping CDA 230 language out of America's trade agreements is critical to our national security. Unfortunately, he chose to turn down Chairman Pallone's invitation and keep the American people in the dark regarding language in trade agreements that has global implications.

I have a long history tracking organized crime and terrorism. For years I worked as a war reporter and wrote a book about the Taliban and the drug trade. As a result of this work, I was recruited by U.S. military leaders to support the intelligence community, where I mapped transnational crime networks for Special Operations Command, the DEA and CENTCOM. In 2014, I received funding from State Department to map wildlife supply chains. That's when my team discovered that the largest retail markets for endangered species are on social media platforms like Facebook and WeChat.

Founding the Alliance to Counter Crime Online has taught me the incredible range and scale of illicit activity happening online. It is far worse than even I ever imagined.

Distinguished members of the committee: The Internet is the new frontier for organized crime and terror groups. We **MUST** get this under control.

Illicit groups have weaponized social media for years now, taking advantage of a market infrastructure that is global, encrypted and highly lucrative.

The tech industry will try and convince you that illegal activity is confined to the dark web.

But surface web platforms provide much the same anonymity as the dark web, as well as payments infrastructure – and a far greater reach of people.

We are in the midst of a public health crisis – the opioid epidemic – which is claiming the lives of more than 60-thousand Americans every year.

Study after study by ACCO members and others have shown widespread use of Google, Twitter, Facebook and YouTube by an estimated 35-thousand illegal online pharmacies to market and sell fentanyl, oxycodone and other highly addictive, often deadly controlled substances to U.S. consumers, in direct violation of federal law.



Facebook, for example, only began tracking drug postings on its platform last year. Within six months, they identified 1.5 million posts selling drugs – and that’s just what they caught.

To put that in perspective, that’s 100 times more postings than the notorious Dark Website the Silk Road ever carried.

Facebook-owned Instagram is today an open marketplace for drug dealers to target teens, and the corporation has never released any data on the volume of drug content on the platform. ACCO researchers have also tracked drug sales on Google, Reddit and Twitter. It’s everywhere.

Why? Because there is no law that holds tech firms responsible, even when a child dies buying drugs on an internet platform.

And it’s not just drug trafficking. Tech firms are removing far less terror content than they claim. Rather, their algorithms connect terror groups like Al Qaeda and Hezbollah to their supporters faster than beleaguered moderators can remove them, and on a wider global scale than these groups could have reached on their own.

ISIS and other terror groups use social media to sell looted artifacts from areas in conflict. ACCO members include an incredible team of Syrian archaeologists recording the online trafficking of thousands of artifacts plundered from ancient sites in their homeland, a war crime under the Second Protocol of the 1954 Hague convention.

We’re now tracking more than 2 million members in 100 active Facebook groups where brokers, including members of terrorist groups, offer loot-to-order services across the Middle East.

Our researchers have identified three additional extremist groups aside from ISIS that are profiting from the sale of stolen artifacts on Facebook and operating with impunity.

We’re tracking groups on Twitter, Instagram, Google and Facebook where endangered species are sold – items ranging from rhino horn and ivory to live cheetahs and apes. In some cases, the size of these markets is literally threatening key species with extinction. Our research, for example, has shown that 70 percent of the annual illegal cheetah trade takes place on Facebook and Instagram.

The black market on social media is far more than just drugs, wildlife, and stolen antiquities. For users who want to watch illegal dog fighting, screen live videos of child exploitation, buy guns, human remains or counterfeit goods, it’s all just a few clicks away.

We support calls for increased user privacy, but current encryption plans laid out by the tech industry will make media platforms even safer for criminals and terrorists.

The tech industry routinely claims that modifying CDA 230 is a threat to freedom of speech.

But CDA 230 is not a law about free speech. It’s about liability.

Try and imagine another industry that has ever enjoyed such an incredible subsidy from Congress: total immunity no matter what harm their product brings to consumers.

Tech firms could have implemented internal controls to prevent illicit activity from occurring but it was cheaper and easier to scale by looking the other way. They were given this incredible freedom, and they have no one to blame but themselves for squandering it.

The “move fast break things” culture developed precisely because of CDA 230.



We want to see reforms to the CDA230 which will remove safe harbor for criminal and terror content. That means:

- Stripping immunities for hosting terror and serious crime content
- Putting the onus on tech firms to monitor their platforms;
- Regulating that firms must report crime and terror activity, along with full data about the users who uploaded it, to law enforcement;
- Appropriating resources to law enforcement to contend with this data.

Distinguished committee members, if it's illegal in real life, it should be illegal to host it online.

It is imperative that we reform CDA230 to make the Internet a safer place for all. Thank you.



alliance to counter crime online

Reports by ACCO submitted as testimony to the House Committee on Energy and Commerce

Subcommittees on Communications and Technology & Consumer Protection and Commerce

Narcotics

Dr. Nilda M. Garcia, "[The Dark Side of Social Media: The Case of the Mexican Drug War](#),"

University of Miami, University of Miami Scholarly Repository, 12/2017.

Dr. Tim Mackey, Jiawei Li, Qing Xu, Neal Shah, "[A machine learning approach for the detection and characterization of illicit drug dealers on Instagram: Model evaluation study](#)," *J Med Internet Res.* 2019 Jun 15;21(6):e13803. doi: 10.2196/13803.

Dr. Tim Mackey, Kalyanam J. [Detection of illicit online sales of fentanyl via Twitter.](#) *F1000Res.* 2017;6:1937.

Dr. Tim Mackey, Kalyanam J, Katsuki T, Lanckriet G. [Twitter-Based Detection of Illegal Online Sale of Prescription Opioid.](#) *Am J. Pub Health.* 2017;107:1910-1915.

Dr. Tim. Mackey, Kalynama J, Klugman J, Kuzmenko E, Gupta R. [Solution to Detect, Classify, and Report Illicit Online Marketing and Sales of Controlled Substances via Twitter: Using Machine Learning and Web Forensics to Combat Digital Opioid Access.](#) *J Med Internet Res.* 2018;20(4):e10029.

Dr. Tim Mackey. Opioids and the Internet: [Convergence of Technology and Policy to Address the Illicit Online Sales of Opioids.](#) *Health Serv Insights.* 2018 14;11:117863291880099.

Antiquities

Dr. Amr al-Azm, Katie Paul, "[Facebook's Black Market in Antiquities](#)," ATHAR Project, June 2019.

See also:

World Politics Review (August 2018) [How Facebook Made it Easier than ever to Traffic Middle Eastern Antiquities](#)

<https://conflictantiquities.wordpress.com/cv/>

Wildlife Crime

Dr. David Roberts and Julio Hernandez-Castro, "[Bycatch and illegal wildlife trade on the dark web](#)," Published online by Cambridge University Press: 14 June 2017.

National Whistleblower's Center, "[Help Stop Wildlife Trafficking on Facebook](#)," April 2018.

See also: WIRED (June 2018): [How Facebook Groups Became a Bizarre Bazaar for Elephant Tusks](#)

Bloomberg (July 2019): [A black market in wildlife trafficking thrives on Facebook and Instagram](#)

Human Remains

Dr. Shawn Graham and Dr. Damien Huffer, "[The Insta-Dead: The rhetoric of the human remains trade on Instagram.](#)" *Internet Archaeology* 45, 2018.

See also: Vice (July 2018): [These Popular Instagram Accounts Are Selling Human Remains](#)

Media and Other Published Reports

Narcotics:



alliance to counter crime online

Ahmed Al-Rawi, "[The fentanyl crisis & the dark side of social media](#)," School of Communication, Faculty of Communication, Art and Technology, Simon Fraser University, 8888 University Drive, British Columbia V5A 1S6, Canada

Sarah Frier, "[Facebook's Crisis Management Algorithm Runs on Outrage](#)," Bloomberg, March 2019.

Romance Scams

Jack Nicas, "[Facebook Connected Her to a Tattooed Soldier in Iraq. Or So She Thought](#)," New York Times, 28 July 2019.

Child Abuse

Michael Keller and Gabriel Dance, "[The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?](#)"