July 13, 2022

To Chairman Peters, Ranking Member Portman, Chairman Durbin, and Ranking Member Grassley:

As privacy, civil rights and civil liberties advocates, we write to urge the Homeland Security & Government Affairs Committee and Judiciary Committee to address the overbroad authority and insufficient protections in the administration's proposed legislation expanding of government power to counter malicious drones. The proposal's authorization for counter-drone activities — including tracking, monitoring, disrupting or bringing down drones that could pose security threats — lacks a sunset, fails to include basic checks on the powers it would convey, and would provide sweeping immunity from all provisions of US Code Title 18.

We recognize the threat this proposal seeks to address is legitimate. However, the proposed measure fails to include basic safeguards for privacy and due process rights, or to protect First Amendment-protected activities from infringement. Among the objectionable aspects of the proposal are the following, which needlessly endanger rights and do not serve to advance government needs for countering malicious drones.

Removal of sunset undermines oversight: Congress established existing authorities to counter drones with a four-year sunset. This was a wise measure. Drones are still a relatively new technology, and are evolving in terms of their capabilities and uses to the public. Counter-drone techniques involve even newer, more uncertain technologies that are still-evolving. Periodic review is essential to ensure that rules created at this time do not improperly inhibit future uses that could provide significant public benefit but are currently unimagined, and do not grant authorities that are broader than necessary. For example, if in the future communications interference is an ineffective detect and counter-drone technology compared to other means, there would be no reason for Congress to permit exceptions to wiretap authorities. Unfortunately, the proposal removes the sunset, risking permanent adoption of rules that will not fit with how drones are used going forward, and setting insufficient oversight of government powers to monitor, damage, and seize private property.

No protection for First Amendment-protected activities: The proposal sets no requirements for agencies to establish rules and standards to safeguard First Amendment-protected activities. It does not direct that constitutional rights be considered as part of the "risk-based assessment" that it requires the agencies to conduct, or require that agencies take steps to minimize risk to First Amendment-protected activities.

This is particularly dangerous as drones have become a valuable tool for journalists, as well as activists recording activities such as protests to spread awareness and document potential police mistreatment of demonstrators. We have seen law enforcement abuse their authority to block drone flights purely for the purpose of stopping reporters from recording the behavior of police,[1] and this proposed text would give the authorities broad latitude to engage in such abuse while providing no means of challenge or redress. It is unacceptable that an investigative journalist or protester might have a drone they are using in a lawful manner for First Amendment-protected activities abruptly taken out of the air due to lax or unclear rules.

Vague authorities create risk of overbroad application or abuse: The proposal gives agencies the ability to set their own bounds on how broadly they can bypass existing statutes for counter-drone activities.

[1] See, Jack Gillum, Associated Press, "AP Exclusive: Ferguson no-fly zone aimed at media," November 2, 2014, available at https://apnews.com/article/674886091e344ffa95e92eb482e02be1.

Specifically, it tasks agency heads with defining what constitutes "credible threat," and broad authority to designate "covered facility or asset." Giving agencies the ability to create their own authority — rather than building clear definitions in statute, establishing a rulemaking process, or providing avenues of redress for improper agency standards — will likely cause development of overbroad standards, and heighten risks that individuals' privacy and due process rights will unnecessarily be infringed.

Overbroad authority to retain private data: The proposal creates exceptions to the 180-day retention limit for data so broad that they effectively subsume the rule. Existing authorities allow government agencies to retain data beyond the limit whenever necessary for an investigation or to support ongoing security operations, an ample authority for preserving data for any legitimate security needs. Despite this, the proposal adds a new exception for retaining data whenever the agency head claims retention protects against unauthorized drone activity, a standard that could allow for virtually limitless retention of data. This is a serious problem given the importance of retention limits for protecting privacy and preventing abuse. It is also a problem given that we do not know how drone technology may evolve in the future, and what kinds of data may become available to government agencies through these authorities.

Augmenting this concern, the proposal grants the Department of Homeland Security (DHS) the authority to create a new government database of security-related incidents involving drones. What constitutes an "incident," what information would be stored, who would have access to that information, how it will be used, and how long it will be retained is completely up to the Secretary of DHS. This blanket authority will likely create a database that is over inclusive and used for purposes beyond the initial reason for its creation.

Blanket immunity needlessly creates risk: The government's legitimate need for counter-drone authority is borne from government claims that these techniques require interception of wireless signals in a manner that would otherwise violate the Electronic Communications Privacy Act. Yet rather than request a specific exemption based on this need, the proposal includes a blanket exemption from *all* of Title 18 of US Code. Blanket immunity from all of Title 18 needlessly gives agencies a blank check, inviting abuse.

Pre-emption of state open-records laws: The proposal would exempt details about the operation of counter-drone technology from state open-records laws. Any temporary advantages of such secrecy for law enforcement are dramatically outweighed by the importance in a democracy of allowing communities to understand what surveillance and other police technologies are being deployed by local authorities, and how, through the open-records laws that they have enacted.

We strongly urge Congress to take steps to remedy these issues, and enact counter-drone legislation that effectively protects privacy, civil rights and civil liberties as well as addressing public safety concerns.

Sincerely,
Advocacy for Principled Action in Government
American Civil Liberties Union
Arab American Institute
Center For Democracy & Technology
Defending Rights & Dissent
Demand Progress
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center

Fight for the Future
Government Information Watch
Open The Government
Project On Government Oversight
Reporters Committee for Freedom of the Press
Restore The Fourth
Surveillance Technology Oversight Project - S.T.O.P.

CC: Members of the Senate Homeland Security and Government Affairs Committee; Members of the Senate Judiciary Committee