

July 25, 2023

TO Chair Peters, Ranking Member Paul, Chair Durbin, and Ranking Member Graham:

As privacy, human rights, civil rights and civil liberties advocates, we write to express our opposition to S.1631, The Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act. While malicious drone activities are a legitimate threat, the bill provides overbroad authority for takedowns, inadequately protects First Amendment and press activities, does not include due process protections for improper counter-drone activities, and lacks basic transparency rules to facilitate responsible use.

We recognize that the government has a genuine need for counter-drone monitoring and mitigation powers. However, given the expanding use of drones by the public—notably by journalists and activists—it is critical that those powers are carefully tailored, and that checks and oversight mechanisms exist to prevent misuse. Unfortunately, S.1631 fails to provide these safeguards. In particular, the bill has the following serious issues:

Inadequate protection for First Amendment-protected activities: The bill fails to set adequate safeguards for First Amendment-protected activities and other constitutional rights. Agencies conducting counter drone activity would not be required to adopt any specific rules or measures to safeguard 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. Law enforcement has already abused their authority to block flights purely to stop reporters from recording the behavior of police.¹ This bill would give the authorities broad latitude to engage in similar suppression of press, without any 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.

No requirement to engage in least-invasive methods: Augmenting this concern, the bill does not require that counter-drone activities undertaken be the least invasive means of responding to a threat. Necessary counter-drone measures can range significantly depending on the situation - sometimes merely identifying the owner of a drone or notifying its operator that it is in a restricted airspace is sufficient to stop a threat. Authorizing personnel only to take the least-intrusive measures reasonably necessary to mitigate a potential threat—and promoting the development of guidelines on how to evaluate threats and necessary responses across various situations—is a commonsense rule that would still permit counter-drone activities that are necessary, while removing the danger of sloppy and overbearing mitigation measures, or even worse, abusive use of counter-drone powers to disrupt journalists' or activists' drones based on the pretext of a threat. Such a measure is particularly critical for any legislation, such as this bill, that seeks to dramatically expand the personnel authorized to engage in counter-drone activities to include not just federal officials, but state and local law enforcement as well.

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>.

Inadequate transparency and reporting measures: The bill fails to require basic reporting measures, such as data on the type and number of detection and mitigation activities conducted pursuant to the authority, or summaries of the results and impact of those activities. Perhaps even more troublingly, it does not require reporting of noncompliance events, any information on whether any drones whose operations were disrupted were engaged in First Amendment-protected activities, or whether any unmanned aircraft systems or unmanned aircraft were improperly seized, disabled, damaged, or destroyed. Such reporting requirements would not compromise methods and techniques, and would be vital protection against abuse. They also would provide the public and policymakers useful information on how counter-drone systems function, and how they might be improved in the future.

No due process or recourse for improper counter-drone activities: The bill provides no due process mechanisms or means of recourse for individuals in the event of counter-drone activity that is improper or of questionable legitimacy. Such actions could result in harm to persons or property—both of a drone operator as well as bystanders—but individuals are given no means of contesting their impropriety or of redress for damage that occurs. Additionally, the bill would make any drone subject to asset forfeiture, regardless of the severity of the violation or maximum penalties that would otherwise be imposed. Asset forfeiture can be a corruptive practice that creates incentives for abuse, and should not be expanded into this field; counter-drone measures should be based on safety and necessity, not on a desire to seize a drone that has flown off course.

Overbroad authority to retain private data: The bill creates an exception to the 180-day retention limit for data so broad that it subsumes the rule. Currently the retention rule is subject to an exemption whenever necessary for an investigation or to support ongoing security operations, providing 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. Blanket indefinite retention is unnecessary, and especially problematic given that drone technology and drone use may evolve unpredictably in the future, and make more revealing data available to government agencies through these authorities.

Pre-emption of state open-records laws: The bill 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 hope Congress will take effective action on this important issue. However, it must do so in a careful manner that protects privacy, human rights, civil rights, and civil liberties, as well as addressing public safety concerns. We urge you to only pass legislation that remedies the issues described above, and ensures that counter-drone authorities are wielded responsibly.

Sincerely,

Advocacy for Principled Action in Government
American Civil Liberties Union
Amnesty International USA
Center for Democracy & Technology
Center for Protest Law & Litigation
Defending Rights & Dissent
Electronic Frontier Foundation
Electronic Privacy Information Center
Fight for the Future
Freedom of the Press Foundation
Government Information Watch
New America's Open Technology Institute
Organization for Identity & Cultural Development
PEN America
Project On Government Oversight
Restore The Fourth
Surveillance Technology Oversight Project (STOP)

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