OTI Opposes the Preventing Emerging Threats Act of 2018 (S. 2836)

The Preventing Emerging Threats Act of 2018 (S. 2836) is a classic case of the medicine being worse than the sickness. While it seeks to address a legitimate concern–the security threat that drones may pose to government facilities–it would threaten Americans' civil liberties and property rights. S. 2836 would confer sweeping authorities on the Departments of Justice (DOJ) and Homeland Security (DHS) to define *when* a drone poses a threat to "covered facilities," and then to surveil, seize, or destroy any drone it determines meets that definition.

- **The scope of S. 2836 is poorly defined, and as such, is dangerously overbroad.** The bill would grant vast authorities to DOJ and DHS if they determine that a drone poses a "threat" to a "covered facility." However, the bill does not define what would constitute a "threat," and imposes no requirement that it be imminent or that it involve a risk to life or safety. Instead, the bill would leave it up to DOJ and DHS to define threats, in consultation with the Department of Transportation. The bill does not even require that the government develop set criteria; as written, it would permit the government to determine that a drone poses a threat on an ad hoc basis.

  Additionally, the bill's definition of "covered facility" is exceptionally broad and includes airspace that is not under any flight restriction and that is not directly above the federal government's property or buildings. It authorizes the government to surveil, seize, or destroy any drone it deems to be a threat and that is flying at the border; over mass gatherings such as protests, parades, concerts, sports events, and other occasions where large numbers of individuals might convene; and around "active Federal law enforcement investigations, emergency responses, or security operations." This would threaten the First Amendment rights of videographers, journalists, drone hobbyists, and average Americans. The authorization could even pose a physical safety threat to individuals in those areas since the government's capability to use force to destroy a drone in a secure manner is unproven.

- **S. 2836 would authorize warrantless surveillance and hacking whenever the government claims a drone poses a "threat" to a "covered facility" and that action is "necessary to mitigate the threat."** This bill would exempt the DOJ and DHS from the requirements of federal criminal law in Title 18 of the U.S. Code. This would permit the warrantless interception or collection of communications that would otherwise be in violation of the requirements of the Wiretap Act and the Stored Communications Act. It would also exempt the government from the Computer Fraud and Abuse Act, which prevents the government from warrantlessly hacking Americans' devices.

- **S. 2836 would authorize the government to seize or destroy a drone without adequate due process.** The bill would authorize DOJ and DHS to seize or use force to destroy any drone that they claim poses a threat to a "covered facility." The bill does not require the government to obtain judicial authorization before seizing or destroying an American's property, and does not contemplate post-hoc review to prevent abuse of this expansive authority. The bill offers no mechanism for accountability or recompense to anyone whose property has been improperly seized or destroyed.

- **S. 2836's "privacy protections" are superficial and ineffective.** While the bill states that "the interception or acquisition of, or access to, communications to or from" a drone must be "conducted in a manner consistent with the Fourth amendment," its blanket exception to the Wiretap Act and the Stored Communications Act, and its expansive authority to warrantlessly seize or destroy Americans' property are anathema to that protection. Additionally, once the government has warrantlessly intercepted communications, those communications would be subject to sweeping exceptions to the two privacy protections included in the bill: that their sharing be limited and that they be deleted after 180 days. Once collected, this bill would allow communications to be shared without limit if sharing them is necessary to further any function of DOJ or DHS, or if the communications could support any criminal, civil, or regulatory investigation by any other government agency. Those communications could also be stored indefinitely if it is deemed necessary to support DOJ, DHS, or any other civilian law enforcement agency's functions.

For more information, contact Robyn Greene, Policy Counsel and Government Affairs Lead, New America's Open Technology Institute, at greene@opentechinstitute.org.