epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Submission of the

ELECTRONIC PRIVACY INFORMATION CENTER

to the

UN SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION

The Surveillance Industry and Human Rights

February 13, 2019

The Electronic Privacy Information Center (EPIC) writes in response to the call for submissions on the surveillance industry and human rights, undertaken by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.[1] Specifically, the Special Rapporteur seeks information about "domestic regulatory frameworks governing the development, marketing, export, deployment, and or facilitation of surveillance technologies by private companies" and information "concerning the use of such surveillance technologies" by states.[2] EPIC submits the following information for study to the Special Rapporteur: (1) recent developments in U.S. export controls for private surveillance technologies, (2) corresponding limits on domestic access to that technologies, and (3) paradigmatic examples of state use.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age.[3] EPIC frequently testifies before the U.S. Congress,[4] participates in the U.S. administrative agency rulemaking process,[5] and

---

[1] UN Special Rapporteur on Freedom of Expression, *Call for Submissions: The Surveillance Industry and Human Rights*, Freedex.org (Dec. 13, 2018), https://freedex.org/2018/12/13/call-for-submissions-the-surveillance-industry-and-human-rights/.
[2] *Id.*
[3] *See*, EPIC, *About EPIC,* EPIC.org*, https://epic.org/epic/about.html.*
[4] EPIC, *EPIC Congressional Testimony and Statements,* EPIC.org*,* https://epic.org/testimony/congress/.
[5] EPIC, *EPIC Administrative Procedure Act (APA) Comments,* EPIC.org*,* https://epic.org/apa/comments/.

litigates landmark privacy cases.[6] EPIC has played a pivotal role in the international development of privacy law and policy. EPIC established the Public Voice project in 1996 to enable civil society participation in decisions concerning the future of the Internet.[7] EPIC also publishes *Privacy and Human Rights*, a comprehensive review of privacy laws and developments around the world, and the *Privacy Law Sourcebook*, which includes many of the significant privacy frameworks.[8]

I. Export Controls for Private Surveillance Technologies

Three recent developments in U.S. export controls may significant effect private surveillance technologies and human rights. First, the U.S. Commerce Department may propose new export controls designed to protect human rights. Second, the U.S. is undertaking a broad review of export controls for new technologies. Finally, the U.S. has thus far delayed adoption of 2013 amendments to the Wassenaar List.

First, the U.S. Commerce Department reportedly plans to propose new export controls intended to safeguard human rights.[9] The U.S. Congressional-Executive Commission on China sent a letter to the Commerce Department in September 2018 urging the agency to limit the "sale by U.S. companies of surveillance and crime control technology for use by Chinese security forces and police."[10] The Commission letter was motivated by the "pervasive surveillance and internment system targeting Uyghurs and other predominantly Muslim ethnic minorities in the Xinjiang Uyghur Autonomous Region (XUAR)."[11] While no proposed rule has yet been published, the Secretary reportedly responded that the Commerce Department plans to seek "human rights controls for the 21st century."[12]

---

[6] EPIC, *Litigation Docket,* EPIC.org*,* https://epic.org/apa/comments/ https://epic.org/privacy/litigation/#cases.
[7] *See*, *About the Public Voice*, The Public Voice, http://thepublicvoice.org/about-us/.
[8] EPIC, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (ed. M. Rotenberg EPIC 2006) and EPIC, *The Privacy Law Sourcebook 2018: United States Law, International Law, and Recent Developments* (ed. M. Rotenberg EPIC 2018), available at: https://epic.org/bookstore/.
[9] Patricia Zengerle, *China may face more U.S. export restrictions over Muslim crackdown*, Reuters (Oct. 2, 2018), https://www.reuters.com/article/us-china-xinjiang-usa/china-may-face-more-u-s-export-restrictions-over-muslim-crackdown-idUSKCN1MC2QD.
[10] Letter from Senators Marco Rubio & Chris Smith to Sec'y of Commerce Wilbur Ross (Sept. 12, 2018), https://www.rubio.senate.gov/public/_cache/files/45fbf9dc-db1d-49d3-9d70-d119e2aa332e/057DC6F80AB6958BF396FC989F5000E5.commerce-end-user-restrictions-sept-12-2018-002-.pdf.
[11] Letter from Senators Marco Rubio & Chris Smith to Sec'y of Commerce Wilbur Ross (Sept. 12, 2018), https://www.rubio.senate.gov/public/_cache/files/45fbf9dc-db1d-49d3-9d70-d119e2aa332e/057DC6F80AB6958BF396FC989F5000E5.commerce-end-user-restrictions-sept-12-2018-002-.pdf.
[12] Peter Lichtenbaum, David W. Addis, & Doron O. Hindin, *Cyber-surveillance export control reform in the United States*, WorldECR ,1, 2 Dec. 2018, at 3-4., https://www.cov.com/-/media/files/corporate/publications/2018/12/cybersurveillance_reform_in_the_united_states.pdf.

The Commerce Department is simultaneously undertaking a broad review of export controls for new technologies. At the end of 2018, Congress passed the Export Control Reform Act of 2018 as a part of the National Defense Authorization Act (NDAA) for Fiscal Year 2019.[13] The law empowers the Department of Commerce to set new controls on both "emerging" and "foundational" technologies for national security purposes. The Department recently solicited public comment concerning what technologies qualify as "emerging" technologies essential to U.S. national security.[14] The agency prompt suggests AI and machine learning technology, data analytics technology, quantum information and sensing technology, robotics such as micro-drone systems, and advanced surveillance technologies such as faceprint and voiceprint technology may be subject to controls.[15] Commerce has not yet published a final rule, nor has it yet called for comment on "foundational" technologies.

Finally, the U.S. has thus far not implemented domestic regulations for export control "intrusion software" and "IP network communications surveillance systems," added to the Wassenaar List in 2013. The Wassenaar Arrangement is an arrangement of forty-two countries, including the U.S., most European nations, India, Turkey, Argentina, South Africa, and Russia. restricting exports of arms and dual-use technology to prevent destabilizing military capabilities.[16] The deal is updated annually and in 2013 "intrusion software" and "IP network communications surveillance systems" were added to the list of restricted technologies,[17] intended to address revelations that Western surveillance technology was being used by repressive regimes.[18] The U.S. implements the deal through administrative rules which often do not mirror, but reflect the spirit, of the language of the Agreement.[19] When the Commerce Department solicited public comment on a proposed implementing rule,[20] both the rule and the Wassenaar updates were heavily criticized by cyber security researchers and civil society as overbroad rule who contended licensing requirements would significantly compromise the security flaws research preserves security.[21] The Department of Commerce withdrew the rule

---

[13] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No: 115-232 (2018).
[14] Bureau of Indus. and Sec'y, "Review of Controls for Certain Emerging Technologies," 83 Fed. Reg. 58201 (Nov. 19, 2018).
[15] *Id*.
[16] *About Us*, The Wassenaar Arrangement, https://www.wassenaar.org/about-us/.
[17] *Id.*
[18] Garrett Hinck, *Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research*, Lawfare (Jan. 5, 2018), https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research; Trevor Timm & Jillian C. York, *Surveillance Inc: How Western Tech Firms Are Helping Arab Dictators*, Atlantic (Mar. 6, 2012), https://www.theatlantic.com/international/archive/2012/03/surveillance-inc-how-western-tech-firms-are-helping-arab-dictators/254008/.
[19] Peter Lichtenbaum, David W. Addis, & Doron O. Hindin, *supra* note 12, at 2.
[20] Bureau of Indus. and Sec'y, "Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items," 80 Fed. Reg. 28853 (May 20, 2015).
[21] Garrett Hinck, *supra* note 19.;Privacy International, BIS Submission (2018), https://privacyinternational.org/sites/default/files/2018-02/Privacy%20International%20BIS%20submission.pdf.

and decided not to implement these new provisions of the Wassenaar Arrangement. [22] The U.S. subsequently negotiated new research uses to exemptions on the new terms of the Wassenaar Agreement in 2017, clarifying that "vulnerability disclosure" and "cyber incident response" technologies as well as general software updates and upgrades are not controlled by the changes.[23] These initial revisions were largely welcomed by critics.[24] Thus far, the U.S. has still not proposed rules to implement the new categories.

The human rights implications of export controls are not clean cut. Limiting export of surveillance technologies to repressive regimes can have intended (where aimed at human rights) or unintended (where the target is national security) benefits when appropriately tailored to the problem. On the other hand, as evidenced by the U.S. debate over the 2013 Wassenaar updates, well intentioned controls that are imprecisely drafted may compromise other rights supporting public goods like cybersecurity. Judgment about the relative human rights merits of the above regulatory processes should be suspended until a proposed regulation is released.

II. Limits on Domestic Access to Private Surveillance Technologies

As to domestic regulation of domestic access to private surveillance technologies, U.S. law bans civilian access to certain private surveillance technologies. Government acquisition is often opaque and nonrestrictive.[25]

The U.S. law imposes narrow but strict limits on civilian access to certain surveillance technologies. For instance, the Wiretap Act Section 2512 prohibits the manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices, except to a domestic U.S. communications service provider or a federal, state or local U.S. government agency. [26] Similarly, the Communications Act of 1934 prohibits the operation of

---

[22]Letter from Sec'y of Commerce Penny Pritzker to Business Associations (Mar. 1, 2016), https://static1.squarespace.com/static/55c4b54ae4b052707386ef7d/t/57716ab31b631bf0f301a81b/1467050675480/Response+from+Secretary+Pritzker+to+Industry+Letter.pdf; Shaun Waterman, *The Wassenaar Arrangement's latest language is making security researchers very happy*, CyberScoop (Dec. 20, 2017), https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/.

[23] Bureau of Indu. Sec., Dep't of Commerce, *FAQs - 1. What changes were made to the Wassenaar Arrangement list in 2017 for intrusion software and why were they made?*, Bis.doc.gov (Feb. 13, 2018), https://bis.doc.gov/index.php/2011-09-12-20-18-59/export-and-reexport-faqs/faq/62-1-what-changes-were-made-to-the-wassenaar-arrangement-list-in-2017-for-intrusion-software-and-why-were-they-made.

[24]Letter from Sec'y of Commerce Penny Pritzker to Business Associations (Mar. 1, 2016), https://static1.squarespace.com/static/55c4b54ae4b052707386ef7d/t/57716ab31b631bf0f301a81b/1467050675480/Response+from+Secretary+Pritzker+to+Industry+Letter.pdf; Shaun Waterman, *The Wassenaar Arrangement's latest language is making security researchers very happy*, CyberScoop (Dec. 20, 2017), https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/.

[25] *See* Catherine Crump, *Surveillance Policy Making By Procurement*, 90 Wash. L. Rev. 1595 (2016), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3637&context=facpubs.

[26] 18 U.S.C. § 2512.

"cell jammers" – devices that are designed to block, jam, or otherwise interfere with radio transmissions.[27] Federal law also prohibits marketing or sale of these devices except to the government.[28] Willful or malicious interference with government or satellite communications is a criminal act.[29]

On the other hand, federal and state law enforcement procurement of private surveillance products is commonplace in the U.S., and acquisition of surveillance tech may be, at best, buried in procurement databases.[30] It is often transferred to local law enforcement agencies without oversight by local officials or the public.[31] In fact, domestic law enforcement have been required not to disclose the use of new surveillance technologies in use.[32] For instance, FBI entered into non-disclosure agreements with local police departments requiring the use of "'additional and independent investigative means and methods' to avoid revealing " the widespread use of "Stingrays," cell site simulators that collect telephone data.[33] Over the past several years, however, a growing number local governments have passed legislation regulating the acquisition of new surveillance technology.[34] Cambridge, Massachusetts passed the most recent iteration in December 2018 - the "Surveillance Technology Ordinance."[35] The Ordinance requires City Council approval before seeking funding, acquisition, or use of a new surveillance technology. The agency is required to submit an "Impact Report" to the City Council for approval, setting out how the technology will be used and where and the potential impact on rights.

III. Paradigmatic Examples: Government Use of Private Surveillance Technologies

The two ongoing EPIC Freedom of Information Act lawsuits described below are paradigmatic examples how the state relies on private sector to supply surveillance technologies - both for new law enforcement field devices (e.g. Cellebrite's mobile forensics) and for analytical databases to crunch vast amounts of data collected about individuals (e.g. Palantir's data analytics). Other cases EPIC is currently pursuing seek details of a homeland security

---

[27] 47 U.S.C. §§ 301, 333.
[28] 47 U.S.C. § 302.
[29] 18 U.S.C. §§ 1362, 1367(a).
[30] Justin Rohrlich & Dave Gershgorn, *The DEA And ICE Are Hiding Surveillance Cameras in Streetlights,* Gov't Exec. (Nov. 9, 2018), https://www.govexec.com/contracting/2018/11/dea-and-ice-are-hiding-surveillance-cameras-streetlights/152734/.
[31] Crump, *supra* note 25, at 1597.
[32] Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal* Cases (2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases#.
[33] *Id.*
[34] Robyn Greene, *How Cities Are Reining in Out-of-Control Policing Tech*, Slate (May 14, 2018), https://slate.com/technology/2018/05/oakland-california-and-other-cities-are-reining-in-out-of-control-police-technologies.html; *see also* Community Control Over Police Surveillance– Guiding Principles (2016).
[35] Ord. No. 1402 "Surveillance Technology Ordinance," http://2f8dep2znrkt2udzwp1pbyxd-wpengine.netdna-ssl.com/wp-content/uploads/2018/12/CambridgeSurveillanceOrdinanceSnapshot-39648.pdf.

media monitoring program,[36] drone surveillance procedures,[37] and the roll out of facial recognition technology at airports.[38]

Cellebrite - Mobile Forensics

Immigration and Customs Enforcement (ICE) is a component law enforcement agency of the Department of Homeland Security (DHS). The agency enforces federal border laws and conducts homeland security investigations, operating both at the U.S. border and the interior. ICE's law enforcement activities include conducting warrantless electronic device searches "without individualized suspicion,"[39] -and recently signed contracts with Cellebrite, a provider of mobile forensic technology.[40] Cellebrite sells Universal Forensic Extraction Devices (UFED) which unlock, decrypt, and extract phone data, including "real-time mobile data . . . call logs, contacts, calendar, SMS, MMS, media files, apps data, chats, passwords."[41] According to Cellebrite, the "UFED Cloud Analyzer tool" can extract private information—even without the assistance of the owner—from private cloud based accounts, such as those maintained by Facebook, Gmail, iCloud, Dropbox, and WhatsApp.[42]

EPIC filed a Freedom of Information Act lawsuit against ICE in April 2018 to obtain details of the agency's use of mobile forensic technology in warrantless searches.[43] EPIC seeks disclosure of contracts for purchase of the technology, policies and procedures on of the mobile data forensics technology at the border and in the US interior, and any privacy and civil liberties assessments.[44]

Palantir - Analytical Databases

---

[36] EPIC, *EPIC v. DHS (Media Monitoring Services)*, Epic.org, https://epic.org/foia/dhs/media-monitoring-services/.
[37] EPIC, *EPIC v. DHS (Drone Policies)*, Epic.org, https://epic.org/foia/dhs_2/epic_v_dhs_drone_policies.html.
[38] EPIC, *EPIC v. CBP (Biometric Entry/Exit Program)*, Epic.org, https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html.
[39] U.S. Immigration and Customs Enforcement, Directive No. 7-6.1 Border Searches of Electronic Devices (Aug. 18, 2009), https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.
[40] Search Results 'Cellebrite PIID:"HSCEMD17P00012"' Feb. 11, 2019, https://www.fpds.gov/ezsearch/search.do?q=Cellebrite+PIID%3A%22HSCEMD17P00012%22&s=FPDSNG.COM&templateName=1.4.4&indexName=awardfull&sortBy=OBLIGATED_AMOUNT&desc=Y.
[41] Cellebrite Mobile Forensics, Unlock Digital Intelligence: Accelerate Investigations Anywhere (2015), https://web.archive.org/web/20170614063253/https://www.cellebrite.com/Media/Default/Files/Forensics/Solution-Briefs/Mobile-Forensics-Solution-Brief.pdf.
[42] *See* Cellebrite, *UFED Cloud Analyzer: Unlock cloud-based evidence to solve the case sooner*, Cellebrite, https://www.cellebrite.com/en/products/ufed-cloud-analyzer/.
[43] Complaint, *EPIC v. ICE,* No. No. 18-cv-00797 (D.D.C. Apr. 9, 2018), https://www.epic.org/foia/ice/mobile-forensics/1-Complaint.pdf.
[44] *Id.*

ICE has also contracted with data mining firm Palantir Technologies, Inc. ("Palantir") to establish and manage key agency information systems. The systems "FALCON" and "ICM" are designed to make determinations about specific, identifiable individuals. Palantir is a data-mining firm that takes personal data and, applying proprietary techniques, makes determinations about their fitness for employment, travel, and whether they should be targeted for further investigations.[45] Through the FALCON and ICM databases, Palantir software allows ICE to access and crunch vast amounts of personal data across numerous federal databases.[46] While both systems collect a significant amount of personal information, the agency exempted these systems from many protections of the Privacy Act.

EPIC filed a Freedom of Information Act lawsuit for records about ICE's contracts and other information related to the FALCON and ICM systems.[47] EPIC is seeking the government contracts with Palantir, any agency assessments, and other related documents. A previous lawsuit brought by EPIC revealed that Palantir played a role in operating "Analytical Framework for Intelligence" for another DHS component, a system which assigned "risk assessments" to travelers.[48]

IV. Conclusion

EPIC welcomes the UN Special Rapporteur study of the relationship between the private surveillance industry and human rights. We look forward to release of the report to the General Assembly in October 2019.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC International Counsel

[45] *See* Jacques Peretti, *Palantir: the 'special ops' Tech Giant That Wields As Much Real-World Power As Google*, The Guardian (July 30, 2017), https://www.theguardian.com/world/2017/jul/30/palantir-peter-thiel-cia-data-crime-police; Ashlee Vance & Brad Stone, *Palantir, the War on Terror's Secret Weapon*, Bloomberg (Nov. 22, 2011), https://www.bloomberg.com/news/articles/2011-11-22/palantir-the-war-on-terrors-secret-weapon.
[46] *See* Spencer Woodman, *Palantir Enables Immigration Agents to Access Information From the CIA*, The Intercept (Mar. 17, 2017), https://theintercept.com/2017/03/17/palantir-enables-immigration-agents-to-access-information-from-the-cia/.
[47] EPIC, *Epic v. ICE (Palantir Databases)*, Epic.org, https://epic.org/foia/dhs/ice/epic_v_ice_palantir_databases.html.
[48] EPIC, *EPIC v. CBP (Analytical Framework For Intelligence)*, Epic.org https://epic.org/foia/dhs/cbp/afi/.