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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER to the

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

International Internet Policy Priorities

[Docket No. 180124068-8068-01]

July 31, 2018

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the National Telecommunications and Information Administration's ("NTIA") notice of inquiry seeking recommendations for the agency's international internet policy priorities in 2018 and beyond.[1]

EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC also support civil society participation in Internet policy. In 1996, EPIC established the Public Voice project to promotes civil society participation in decisions concerning the future of the Internet.[3] Since that time, EPIC has hosted more than two dozen conferences around the world on topics ranging from cryptography policy and consumer protection to data protection and the digital economy.[4] An upcoming Public Voice conference in Brussels explores "AI, Ethics, and Fundamental Rights."[5] And the EPIC Public Voice Fund provides support for small NGOs to participate in Internet policy work.[6] EPIC also helped establish the Civil Society Information Society Advisory Council, which provides civil society input for the OECD on Internet Policy.[7]

EPIC itself is a leading advocate for consumer privacy. In a recent commentary, we said that the Commerce Department had failed to recognize the importance of privacy protection for the digital economy.[8] As we wrote in the *Financial Times*, "Instead of criticizing the EU effort, the

---

[1] NTIA, *International Internet Policy Priorities*, Notice of Inquiry, Docket No. 180124068-8068-01 (June 5, 2018), https://www.ntia.doc.gov/federal-register-notice/2018/notice-inquiry-international-internet-policy-priorities.

[2] EPIC is a non-partisan research and advocacy center in Washington, DC. EPIC's members include distinguished experts in law, technology, and public policy. About EPIC, https://epic.org/epic/about.html.

[3] The Public Voice, http://thepublicvoice.org/.

[4] The Public Voice -Events, http://thepublicvoice.org/events/

[5] "AI, Ethics, and Fundamental Rights," October 23, 2018, Brussels, Belgium, http://thepublicvoice.org/events/brussels18/

[6] EPIC, Public Voice Fund, https://www.epic.org/epic/publicvoicefund/

[7] CSISAC, ("CSISAC is the voice of civil society at the OECD's Committee on the Digital Economy Policy. We facilitate the exchange of information between the OECD and civil society participants, leading to better-informed and more widely accepted policy frameworks.") https://csisac.org/

[8] Marc Rotenberg, "Congress can follow the EU's lead and update US privacy laws," Financial Times, May 31, 2018, https://www.ft.com/content/39044ec6-64dc-11e8-a39d-4df188287fff.

commerce department should help develop a comprehensive strategy to update US data protection laws."[9]

EPIC advises NTIA to pursue comprehensive data protection legislation that would strengthen privacy protections for Americans and create an independent agency to enforce those rights. Updated data privacy laws would facilitate the free flow of information online. The multistakeholder approach is often is dominated by industry representatives and leads to regulatory capture. We therefore believe a legislative approach will lead to better outcomes for the public.

I. The Free Flow of Information and Jurisdiction

A. What are the challenges to the free flow of information online?

The failure of the U.S. to update its data privacy laws continues to pose a significant challenge to the free flow of information online. Transborder flows of personal data are a bedrock of digital commerce. Particularly in the realm of data protection, baseline privacy standards are often key to facilitating these transfers. For instance, foreign states may require third country hosting data sufficiently protects any data before it is entitled to receive data transfers.[10] As a result, increasing the level of data protection and privacy provided to match the highest global standards available under law is the best means of facilitating free information flow.

The level of privacy protection guaranteed under national law can be undermined if the data is transferred to a less protective legal or regulatory regime. In order to build trust that undergirds free data flow, a high level of legal and regulatory protection and protecting fundamental privacy rights must be maintained regardless of where data travels. *Schrems v. Data Protection Commissioner*, the European Court of Justice's landmark decision striking down the EU-US "Safe Harbor" arrangement is evidence that the failure to adequately consider privacy risks in the global digital ecosystem ends poorly for both human rights and the digital economy.[11]

The Privacy Shield negotiated in its place failed to address the issues with Safe Harbor. Privacy Shield did not address the need for independent oversight and effective remedies for violations of legal rights.[12] Today, the agreement is subject to ongoing legal challenge and risks being struck down.[13] This instability of data flows internationally has long-term negative consequences for free flow of information.

To address this challenge the United States could pursue three options:

---

[9] Marc Rotenberg, *Congress can follow the EU's lead and update US privacy laws*, FINANCIAL TIMES (June 1, 2018), https://www.ft.com/content/39044ec6-64dc-11e8-a39d-4df188287fff.
[10] *See, e.g.*, Regulation 2016/679, 2016 O.J. (L119) 1 (EU).
[11] C-362/14, *Schrems v. Data Prot. Comm'r*, 2015 E.C.R. 650.
[12] *See, e.g.*, Letter from EPIC, et. al, to Isabelle Falque-Pierrotin Chairman, Article 29 Working Party, et. al (Mar. 16, 2016), https://epic.org/privacy/intl/schrems/Priv-Shield-Coalition-LtrMar2016.pdf.
[13] EPIC, *Data Protection Commissioner v. Facebook & Max Schrems (Irish High Court)*, EPIC.org https://epic.org/privacy/intl/DPC-v-Facebook-IrishCourt/ (referral to CJEU includes questions concerning Privacy Shield).

(1) Draft and Enact Comprehensive Privacy Law

(2) Encourage US firms to comply with the GDPR

(3) Ratify the Council of Europe Privacy Convention

(1) Draft and Enact Comprehensive Privacy Law

EPIC has long favored the establishment of comprehensive privacy law in the United Stated.[14] The current mix of sectoral regulation and self-regulation is ineffective, inefficient, cumbersome, and costly. Consumers receive too little actual protection and small firms are the targets of too many lawsuits that provide little actual benefit to those on whose behalf cases are brought. The FTC also lacks the ability, authority and expertise to engage the broad range of challenges we now confront – Internet of Things, AI, connected vehicles, and more. Identify theft and data breaches are at all-time highs.[15] And most critically consumer protection has become a national security concern as foreign adversaries increasingly target the data of personal data of Americans held by US firms and US government agencies.[16]

The NTIA should not ignore this reality or suggest that non-binding principles will do anything to address these real challenges to the digital economy and consumer protection.[17] Comprehensive legislation is long over-due. The United States could take as a starting point, the OECD Privacy Guidelines, which the US helped draft and which more than 200 US firms endorsed.[18] The OECD Privacy Guidelines build on the work of the US Privacy Protection Study Commission and reflect many of the same privacy rights and responsibilities found in the US Privacy Act. [19]

(2) Encourage US Firms to Comply with the GDPR

---

[14] *See, e.g.*, Testimony and Statement of Marc Rotenberg, EPIC President, Hearing on Consumer Data Security and the Credit Bureaus Before the Committee on Banking, Housing, and Urban Affairs United States Senate (Oct. 17, 2018), https://epic.org/privacy/testimony/EPIC-Testimony-SBC-10-17.pdf.

[15] Identity Theft Resource Center, Data Breaches Increase 40 Percent in 2016, Finds New Report (Jan. 19, 2017), http://www.idtheftcenter.org/2016databreaches.html.

[16] *See, e.g.*, 4 Equifax, Equifax Announces Cybersecurity Incident Involving Consumer Information (Sept. 7, 2017), https://investor.equifax.com/tools/viewpdf.aspx; Ellen Nakashima, Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say, Wash. Post (Jul. 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearancesystem-affected-21-5-million-people-federal-authorities-say/.

[17] Remarks of Assistant Secretary Redl at IGF-USA 2018 (July 27, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-igf-usa-2018

[18] EPIC, *EPIC International Privacy Standards*, Epic.org, https://epic.org/privacy/intl/; Remarks of Marc Rotenberg, 30th Anniversary of the OECD Privacy Guidelines, OECD Paris France, (Mar. 10, 2010), http://www.oecd.org/internet/interneteconomy/44946274.doc ("The OECD Privacy Guidelines are the most influential international framework for privacy ever established.").

[19] OECD Privacy Guidelines (2013), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

In the absence of a US privacy law, US firms will still need direction. The NTIA should encourage US firms to comply with the General Data Protection Regulation as many US firms have already done. The GDPR is a modern, comprehensive approach to privacy protection that incorporates privacy safeguards found in US law and many data protection laws around the world.[20] The aim is to promote the free flow of information by ensuring privacy protection. Fairness, accountability, and transparency, all critical to digital economy, are the pillars of the GDPR.

But there is also a very practical reason for the NTIA to back the GDPR – it is efficient and practical for US firms operating in the EU to offer comparable protections for US consumers. In fact, it is not at all clear how US firms could justify offering higher standards of privacy protection to EU consumers than it does to consumers in the United States. The NTIA should give serious thought to this issue. Consumer organizations around the world have already urged US companies to comply with GDPR.[21]

(3) Ratify the Council of Europe Privacy Convention

EPIC urges the NTIA to pursue U.S. ratification of Convention 108 (also referred to as the "International Privacy Convention)." The Privacy Convention is the first binding international legal instrument on data protection, and is open to any country, including non-members of the Council of Europe. The Council of Europe established the Convention in 1981 to strengthen the legal protection of individuals with regard to automatic processing of personal information.[22] The Convention was amended in 2018 to reflect changes in new technology.[23] The Convention now requires prompt data breach notification, establishes national supervisory authorities to ensure compliance, permits transfers abroad only when personal data is sufficiently protected, and provides new user rights including algorithmic transparency.[24]

EPIC has long campaigned for the U.S. to ratify the Privacy Convention.[25] As EPIC recently wrote to Congress:

> The protection of privacy is a fundamental human right. In the 21st century, it may become one of the most critical human rights of all. Civil society organizations form around the

[20] EPIC, *EU General Data Protection Regulation*, Epic.org, https://epic.org/international/gdpr/.
[21] *See, e.g.*, Letter from the Trans Atlantic Consumer Dialogue (TACD) to Mark Zuckerberg, CEO, Facebook (Apr. 9, 2018), http://tacd.org/wp-content/uploads/2018/04/TACD-letter-to-Mark-Zuckerberg_final.pdf; Letter from fourteen Latin American consumer groups to Mark Zuckerberg, CEO, Facebook, and Gareth Lambe, Director, Facebook Ireland (Apr. 18, 2018), https://sontusdatos.org/wp-content/uploads/2018/04/180418-letter_zuckerberg-fv.pdf.
[22] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, ETS No. 108.
[23] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), May 18, 2018, CM(2018)2 https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e.
[24] EPIC, *Council of Europe Modernizes International Privacy Convention*, Epic.org, (May 18, 2018), https://epic.org/2018/05/council-of-europe-modernizes-i.html.
[25] EPIC, *Council of Europe Privacy Convention*, Epic.org, https://epic.org/privacy/intl/coeconvention/.

world have recently asked that countries which have not yet ratified the Council of European Convention 108 and the Protocol of 2001 to do so as expeditiously as possible.[26]

We would also encourage the NTIA to review The Madrid Privacy Declaration. The Madrid Privacy Declaration is a document drafted in 2009 in tandem with the 31st International Conference of Data Protection and Privacy Commissioners.[27] EPIC seeks widespread adoption of the Declaration, which "reaffirms international instruments for privacy protection, identifies new challenges, and call[s] for concrete actions" and has been signed by hundreds of organizations and experts.[28] The Declaration also urges those nations that have not ratified the Privacy Convention to do so expeditiously.[29] The NTIA should consider the priorities of this foundational civil society document as it develops a privacy policy for the 21st century.

II. Multistakeholder Approach to Internet Governance

A. Does the multistakeholder approach continue to support an environment for the internet to grow and thrive? If so, why? If not, why not?

We strongly favor meaningful public input into agency decision-making. In fact, such input is required by law.[30] But the "multistakeholder process" does not produce meaningful outcomes. Though many groups have devoted substantial times to the multistakeholder process, there are few concrete outcomes.

The multistakeholder approach to internet policy also leads quickly to capture as participants seek funding from private sources to participate in meetings.[31] Even agencies themselves are subject to capture as key actors often take positions after they leave government service with companies they would oversee but chose instead to establish a series of multistakeholder proceedings.

EPIC favors democratic decision-making, meaningful public input, the rule of law, finality, and judicial review when it comes to agency decision-making on all issues, including Internet policy.

IV. Emerging Technologies and Trends

[26] Letter from EPIC to U.S. Senate Committee on Foreign Relations (Apr. 13, 2018), https://www.epic.org/EPIC-SFR-Pompeo-April2018.pdf.
[27] The Madrid Privacy Declaration (2009), http://www.thepublicvoice.org/Madrid-declaration/.
[28] *Id.*
[29] *Id.*
[30] 5 U.S.C. § 553(c). The Administrative Procedure Act requires agencies to "give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments with or without opportunity for oral presentation."
[31] The EPIC Public Voice Fund seeks to address this problem.

A. What emerging technologies and trends should be the focus of international policy discussions? Please provide specific examples.

The increased use of algorithmic decision-making, Internet of Things devices, and facial recognition pose privacy and security risks that should be the focus of international policy discussions. It is critical for the international community to develop standards for cross-border law enforcement access to data stored in foreign jurisdictions that comport with data protection and human rights standards.

(1) Algorithmic and Automated Decision-Making – US Should Support Algorithmic Transparency

The proliferation of secret algorithms for governmental and commercial use threatens the exercise of rights that underpin individual autonomy and liberty. Algorithms are often used to make adverse decisions about people. Algorithms deny people educational opportunities, employment, housing, insurance, and credit. Many of these decisions are entirely opaque, leaving individuals to wonder whether the decisions were accurate, fair, or even about them. It is timely to address this now, as reliance on secret algorithms is rapidly increasing on a global scale. For example:

- In the United States, secret algorithms are deployed in the criminal justice system to assess forensic evidence, determine sentences, and even to decide guilt or innocence.[32] Several states use proprietary commercial systems, not subject to open government laws, to determine guilt or innocence. The Model Penal Code recommends the implementation of recidivism-based actuarial instruments in sentencing guidelines.[33] But these systems, which defendants may have no opportunity to challenge, can be racially biased, unaccountable, and unreliable for forecasting violent crime.[34]

- Algorithms are used for social control. The Chinese government is deploying a "social credit" system that assigns to each person a government-determined favorability rating. "Infractions such as fare cheating, jaywalking, and violating family-planning rules" would affect a person's rating.[35] Low ratings are also assigned to those who frequent disfavored web sites or socialize with others who have low ratings. Citizens with low ratings will have trouble getting loans or government services. Citizens with high ratings, assigned by the government, receive preferential treatment across a wide range of programs and activities.

[32] EPIC, *EPIC v. DOJ (Criminal Justice Algorithms)* https://epic.org/foia/doj/criminal-justicealgorithms/; EPIC, *Algorithms in the Criminal Justice System* https://epic.org/algorithmictransparency/crim-justice/.
[33] Model Penal Code: Sentencing §6B.09 (Am. Law. Inst., Tentative Draft No. 2, 2011)
[34] See Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[35] Josh Chin & Gillian Wong, China's New Tool for Social Control: A Credit Rating for Everything, Wall Street J. (Nov. 28, 2016), http://www.wsj.com/articles/chinas-new-tool-forsocial-control-a-credit-rating-for-everything-1480351590.

Therefore, algorithmic transparency is critical to ensuring accountability in the input of an automated decision-making process, as well as the rationale for a specific decision impacting the subject's rights and opportunities.

The U.S. needs a legal framework that protects individuals against algorithmic discrimination, through the right to examine the design, implementation, and consequences of automated processing. NTIA's Internet policy should fundamentally require transparency and accuracy at each processing stage to improve data governance, data quality, and the opportunity to correct hidden bias.[36] People should have the right to invoke remedies and obtain redress from adverse decisions made by algorithms. *Please refer to our response to Question IV.C for detailed recommendations on NTIA's policymaking on algorithmic transparency.*

(2) Internet of Things (IoT) and "Always On" Devices – Strong Privacy and Security Standards should be Established

Today, the biggest threat to privacy and security in consumer products is posed by the Internet of Things. IoT devices track personal data by seamlessly integrating into the consumers' activities and lifestyles. They blend into everyday objects, and are not readily discernible as an internet-connected device with the capacity to sense, collect, and transmit large-scale personal data. IoT technology is encapsulated in small unobtrusive devices, often without a direct user interface like a screen. The vast quantity of data generated by IoT creates the risk that this data could be used for purposes that are either unnecessary to the provision of a given service or not initially disclosed to the consumer. Therefore, the ubiquity of IoT sensors and their amassment of granular data pose significant privacy and safety concerns for consumers.

Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[37] These "always on" devices raise numerous privacy concerns, including whether consumers have granted informed consent to this form of tracking. Even if the owner of an "always on" device has consented to constant, surreptitious tracking, a visitor to their home may not. Manufacturers are not required by regulation to incorporate ambient indicators on the device to alert nearby users that the device is recording. This distorts consumer perception of privacy and security in IoT devices. Consumers may simply assume that their personal information is safe from external attacks, even when manufacturers have not implemented safeguards.[38]

[36] Association for Computing Machinery US Public Policy Council (USACM), *Statement on Algorithmic Transparency and Accountability* (Jan. 12, 2017), *available at* https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf
[37] EPIC Letter to DOJ Attorney General Loretta Lynch, FTC Chairwoman Edith Ramirez on "Always On" Devices (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTCAG-Always-On.pdf.
[38] Serena Zheng, Marshini Chetty, and Nick Feamster, *User Perceptions of Privacy in Smart Homes*, (Feb. 2018), https://arxiv.org/pdf/1802.08182.pdf.

Both the intentional designs and unintentional flaws of IoT devices present risks to consumers. There is an urgent need for regulatory action on IoT privacy and security. Companies have little incentive to maintain strong standards without regulation on the manufacturing and design of IoT products. And consumers do not have enough information to evaluate the privacy and security implications of these products themselves. This market structure has exacerbated the power imbalance between consumers and the companies with which they conduct business. Consumers are unable to make meaningful choices on devices that significantly impact their security and safety. This has alarming implications for many products, such as toys that collect children's data[39] and internet-connected home systems like smoke detectors and security cameras. The prevention of security and data breaches in IoT devices should be critical to NTIA's regulatory strategy going forward.

Therefore, NTIA should establish mandatory privacy and security standards and require certification to these standards before IoT devices are allowed into the market stream. To harmonize the use of cybersecurity standards for international manufacturers, NTIA should coordinate its IoT policy development with strong international guidelines such as the UK Government's "Secure by Design" report.[40]

EPIC agrees with the UK Government's assessment that "there is a need to move away from placing the burden on consumers to securely configure their devices, and instead ensure that strong security is built in by design."[41] The code of practice proposed by the UK government serves as a useful framework for security standards for IoT. In particular, IoT should adopt the following safeguards:[42]

1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security-sensitive data
5. Communicate securely

---

[39] *See, e.g.*, In the Matter of Genesis Toys and Nuance Communications, (2016) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf; Campaign for a Commercial-Free Childhood, *Stop Mattel's "Hello Barbie" Eavesdropping Doll*, (Feb. 2015) http://www.commercialfreechildhood.org/action/shut-down-hello-barbie.

[40] UK Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the cyber security of consumer Internet of Things Report* (Mar. 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.

[41] *Id.*

[42] *Id.*

6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Data protection
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate input data

This guidance necessitates privacy and security enhancing techniques in the form of a code of practice. This baseline regulation would ease the burden currently placed on consumers to safely install, maintain, and dispose of IoT products with limited information on the privacy and security of each control and default setting.

These are smart rules that NTIA should adopt to establish a rights and responsibilities model in IoT that is clear, functional, and measurable in consumer products. NTIA's initiative in IoT would ensure that consumers can safely and confidently embrace new technologies entering the market with the assurance that manufacturers have a common approach on the safeguards for privacy and security.

Please refer to our response to Question IV.C for detailed recommendations on NTIA's policymaking on privacy impact assessments and data minimization as other necessary safeguards to IoT privacy.

(3) Facial Recognition Technology – The Use of this Technology should be Suspended Pending the Establishment of Comprehensive Privacy Safeguards

Facial recognition systems include computer-based biometric techniques that detect and identify human faces.[43] The National Academy of Sciences has stated:

> The success of large-scale or public biometric systems is dependent on gaining broad public acceptance of their validity. To achieve this goal, the risks and benefits of using such a system must be clearly presented. Public fears about using

[43] EPIC, *Facial Recognition*, http://epic.org/privacy/facerecognition/. *See also* John D. Woodward, et al, Rand, *Biometrics: A Look at Facial Recognition* 8-9 (2003), *available at* http://www.rand.org/content/dam/rand/pubs/documented_briefings/2005/DB396.pdf.

> the system, including . . . concerns about theft or misuse of information, should be addressed.[44]

Private companies covertly deploy facial recognition techniques to obtain the identity of unsuspecting individuals. For example, Madison Square Garden deploys facial recognition on attendees at public sporting events for both security and marketing purposes.[45] Commercial deployment of facial recognition is pervasive in the advertising industry. For example, Unilever has utilized facial scanning to measure shoppers' emotional engagement with on-shelf displays.[46]

The use of facial recognition technology by governments also raises serious privacy concerns. The United States Custom and Border Protection ("CBP"), Department of Homeland Security ("DHS"), and the Federal Bureau of Investigation ("FBI") coordinate various programs on facial recognition technology that raise substantial privacy and civil liberties concerns.

Facial recognition technology can be done covertly, even remotely, and on a mass scale. There is little that individuals can do to prevent collection on one's image. Participation in society involves exposing one's face. Governments around the world seek access to images of political organizers to obtain actual identities and to enable investigation and prosecution. Ubiquitous and near effortless identification eliminates individual's ability to control their identities and poses a special risk to the First Amendment rights of free association and free expression, particularly to those who engage in lawful protests.

In particular, Facebook's facial recognition technology works by generating a biometric signature for users who are tagged in photos on Facebook, i.e. using "summary data" from "photo comparisons. "This representation of biometric information, based on the user's facial image, generated by Facebook, is available to Facebook but not to the user. Facebook routinely encourages users to "tag," i.e. provide actual identifying information about, themselves, their friends, and other people they may recognize. Facebook generates unique biometric identifiers and links them to individual users without obtaining meaningful and affirmative consent.[47]

The deployment of commercial facial recognition technology is widely considered an invasion of privacy rights in Canada and Europe:

---

[44] National Academy of Sciences, *Biometric Recognition: Challenges and Opportunities (Report in Brief)* 7 (2010), http://sites.nationalacademies.org/cstb/CurrentProjects/CSTB_059722.
[45] Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, The New York Times, (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html?mtrref=undefined.
[46] Michael Barnett, *Unilever trials in-store facial recognition technology*, Marketing Week, (Mar. 7, 2018), https://www.marketingweek.com/2018/03/07/unilever-in-store-facial-recognition/.
[47] EPIC, In re Facebook and Facial Recognition (2018), https://www.epic.org/privacy/ftc/facebook/facial-recognition2018/.

- The Privacy Commissioner's Office found Facebook "in contravention" of Canada's Personal Information Protection and Electronic Documents Act.[48]
- The EU Article 29 Data Protection Working Party issued an opinion on developments in biometric technologies which states that consent must be obtained for the storage and use of biometric data. [49]
- On October 15, 2012, Facebook disabled its tagging facial recognition practice for users in the European Union, following an investigation by the Irish Data Protection Commissioner.

The disparity of biometric privacy protections afforded for the nationals and residents of the United States due to the lack of safeguards against facial recognition technology is unacceptable. NTIA's international Internet policy should establish strict limitations on commercial biometric data collection, as it has been prohibited by regulators in Canada and the European Union.

NTIA should ensure that commercial actors do not deploy facial recognition techniques until adequate safeguards are established. These safeguards should critically include: (1) subject control over image enrollment, (2) subject control over the processing and identification of images, (3) transparency in the functioning, use, and purpose of the facial recognition system, and (4) independent accountability of the image processing entity.[50]

As such safeguards have not yet been established for U.S. consumers, EPIC would recommend a moratorium on the commercial deployment of facial recognition techniques.[51]

(4) Standards for Cross-Border Law Enforcement Access Should Be Strengthened

The development of mutual, appropriate standards for cross border law enforcement access to data are increasingly important in international policy discussions. If the Administration fails to establish robust privacy standards for law enforcement data transfers, international data flows may be jeopardized. The NTIA should work closely with the State and Justice Departments to establish a stronger global framework for law enforcement access to data in foreign jurisdictions.

Law enforcement increasingly seeks communications data stored outside national borders in domestic criminal investigation because of a global digital communications landscape. However, trans-border data access can conflict with national data protection regimes and international human

[48] Elizabeth Denham, Assistant Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act* (July 16, 2009), http://priv.gc.ca/cfdc/2009/2009_008_0716_e.pdf.
[49] Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* (April 27, 2012), *available at,* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.
[50] In the Matter of Facebook, Inc. and the Facial Identification of Users (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) (Jun. 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.
[51] *Id.*

rights instruments.[52] the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act signed into law in March 2018.[53] The CLOUD Act authorizes law enforcement to order service providers with some connection to their jurisdiction to produce data located abroad. This represents a paradigm shift in the system cross-border access to data in criminal investigations - it authorizes one jurisdiction to order production of data stored in third country, without a layer of judicial or other review in the third country. There is widespread concern about the newly proposed mechanism for cross-border access by law enforcement. Indeed, following a forceful statement by the European Parliament's powerful civil liberties committee,[54] the full European Parliament passed a resolution stating that the EU-U.S. Privacy Shield should be suspended if the U.S. does not enhance privacy protections by September 1, 2018.[55] Both statements cited the CLOUD Act as a paramount concern.

> *The NTIA should work with other federal agencies implementing the CLOUD Act to ensure law enforcement cross-border access to data incorporates human rights standards.*

Given the international dimensions of cross border law enforcement access to data, the individual rights protections of any such system should comport with international human rights standards. The NTIA should coordinate with the State and Justice Departments to ensure cross-border law enforcement access to data includes adequate rights safeguards. EPIC described the safeguards mandated by international law[56] for any regime of electronic surveillance in an *amicus* brief in the now mooted Supreme Court case *United States v. Microsoft*.[57] EPIC encourages the NTIA to heed these standards:

> 1) The terms of surveillance should be "accessible" or publicly available; 2) the scope of surveillance should be reasonably foreseeable; 3) the duration of surveillance must be appropriately restricted; 4) surveillance should be cabined by procedures for storing, accessing, examining, using, communicating and destroying the intercepted data; 5) authorization procedures should ensure regularity of surveillance, and, preferably, should include prior judicial review; 6) post-authorization supervision should ensure proper implementation of the surveillance measures, as well as compliance with the storage, access to, use, processing, communication and destruction of intercept material; and 7) notice and an effective remedy should be provided.[58]

---

[52] Brief for EPIC and Thirty-Seven Technical Experts and Legal Scholars as *Amici Curiae* in Support of Respondent, *United States v. Microsoft*, No. 17-2 (Jan. 18, 2018), https://epic.org/amicus/ecpa/microsoft/US-v-Microsoft-amicus-EPIC.pdf.

[53] Consolidated Appropriations Act, 2018, div. V, Pub. L. No.115-141(2018).

[54] EU-US Privacy Shield data exchange deal: US must comply by 1 September, say MEPs (June 12, 2018), http://www.europarl.europa.eu/news/en/press-room/20180611IPR05527/eu-us-privacy-shield-data-exchange-deal-us-must-comply-by-1-september-say-meps.

[55] Suspend EU-US data exchange deal, unless US complies by 1 September, say MEPs (July 5, 2018), http://www.europarl.europa.eu/news/en/press-room/20180628IPR06836/suspend-eu-us-data-exchange-deal-unless-us-complies-by-1-september-say-meps.

[56] See *e.g.*, *Zakharov v. Russia*, App. No. 47143/06, Eur. Ct. H.R. (2015), C-293/12, Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res., 2014 E.C.R. 238.

[57] Brief for EPIC and Thirty-Seven Technical Experts and Legal Scholars as *Amici Curiae* in Support of Respondent, *supra* note 7, at 26-42.

[58] Brief for EPIC and Thirty-Seven Technical Experts and Legal Scholars as *Amici Curiae* in Support of Respondent, *supra* note 7, at 26-42.

C. What are the current best practices for promoting innovation and investment for emerging technologies? Are these best practices universal, or are they dependent upon a country's level of economic development? How should NTIA promote these best practices?

(1) Algorithmic Transparency

NTIA should assess whether individual rights are protected against algorithmic profiling and discrimination through the right to examine the design, implementation, and consequences of automated processing. The agency should establish checkpoints for transparency and accuracy at each processing stage to improve data governance, data quality, and the opportunity to correct hidden bias.

There must be a U.S. regulatory framework to ensure fairness in automated processing and the right to explanation of the logic of processing. Actionable measures are necessary for individuals to examine the algorithm's "logic process" and the factors contributing to an automated decision, to provide an opportunity to rectify inaccurate information or machine-learning biases. This additional safeguard is critical to the protection of individual rights, because even accurate input can be distorted by a particular analytic model to extrapolate biased inferences that result in profiling and algorithmic discrimination.

International legal frameworks recognize that the touchstone of algorithmic transparency is the responsibility of institutions to justify the provability of their own analytic systems and to address potential and actualized harms. The EU General Data Protection Regulation ("GDPR") establishes legal and regulatory measures to contest automated decisions, and enforcement mechanisms to end opaque practices that threaten fundamental rights.[59]

In the United States, there is growing suppor for Algortithmic Transparency. [DISCUSS]

(2) Privacy Impact Assessments ("PIAs")

Federal agencies are routinely required to conduct a Privacy Impact Assessment prior to the creation of system containing personal data.[CITE – Section 208 E-Governemnt Act.] Conducting a thorough privacy impact assessment ("PIA") is the first step to identifying potential defects that

[59] EPIC Comments to UK Information Commissioner's Office, *Consultation on Data Protection Impact Assessments (DPIAs) Guidance* (Apr. 12, 2018), https://epic.org/algorithmic-transparency/EPIC-ICO-Comment-GDPR-DPIA.pdf.

could compromise the privacy and security of data processing.[60] Privacy assessments are a critical part of assessing the level of intrusiveness that new technologies could have on individual rights and safety. Leading privacy scholars Paul de Hert and David Wright have noted the value of publishing the assessments to demonstrate accountability.[61]

Moreover, EPIC's "Privacy Impact Assessment" initiative is a key component of the organization's long-running open government project and consumer protection work.[62] Most recently, we advised the UK data protection authority on PIAs[63] and urged that assessments should make clear the risks of automated processing of personal data; increase accountability by embedding PIAs into organizational processes; and encourage privacy-enhancing techniques and data minimization to manage risk.

Requiring PIAs promotes internal oversight of legal and regulatory compliance on data protection. PIAs should be required for companies that collect data as a preliminary assessment of the information flows of personal and potentially sensitive data—detailing how the data is processed and maintained in transit and in storage.

For example, IoT manufacturers and technical designers should comprehensively address and explain the complexities of the underlying data processing systems to the relevant regulatory agency. This assessment would help minimize safety risks by requiring manufacturers to understand how their device works, the implications for privacy and security, and to eliminate the potential for unauthorized access or misuse. Oversight of PIAs in IoT manufacturing would serve an important function of preventing hazardous conditions from being designed into the products without sufficient consideration.

Privacy awareness in each stage of data processing is key to monitoring and patching vulnerabilities, minimizing data collection, managing data access, and prohibiting secondary uses of data. If, for example, PIA appraisals indicate that de-identification is not feasible at certain volumes of data, then the company should employ differential privacy methods or encryption. NTIA should

---

[60] David Wright, *Making Privacy Impact Assessment More Effective*, The Information Society, Vol.29:307–315, (2013)

[61] David Wright & Paul de Hert, *Privacy Impact Assessment* (2012), Springer, Law, Governance and Technology Series, Vol. 6. at 27.

[62] EPIC, *EPIC v. FBI - Privacy Assessments*, https://epic.org/foia/fbi/pia/; *See also*, EPIC, *EPIC v. DEA - Privacy Impact Assessments*, https://epic.org/foia/dea/pia/; EPIC, *EPIC v. NSA - Cybersecurity Authority*, https://epic.org/foia/nsa/nspd-54/default.html; EPIC, *EPIC v. Presidential Election Commission*, https://epic.org/privacy/litigation/voter/epic-v-commission/;EPIC, *EPIC Open Government*, https://epic.org/open_gov/; EPIC, *Complaint In re Universal Tennis to the Federal Trade Commission* (May 17, 2017), https://epic.org/algorithmic-transparency/EPIC-FTC-UTR-Complaint.pdf.

[63] EPIC Comments to UK Information Commissioner's Office, *Consultation on Data Protection Impact Assessments (DPIAs) Guidance* (Apr. 12, 2018), https://epic.org/algorithmic-transparency/EPIC-ICO-Comment-GDPR-DPIA.pdf.

set clear rules for mandatory PIAs prior to data processing, so that companies are auditable on how and why they processed personal data.

EPIC makes the following recommendations for NTIA's international policy on organizational PIAs:

- PIAs must be commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information.[64]

- PIAs should be mandatory for new technologies that collect more granular data on individuals or possess the capacity to collect larger quantities of data. PIAs should assess whether the collection of this data is necessary or proportionate. NTIA should prohibit the excessive collection of data that pose a risk to individual rights.

- NTIA should require organizations to implement technical and operational measures to allow individuals to scrutinize PIAs and exercise their rights accordingly.

- Whenever there is automated processing of data, PIAs should provide for algorithmic transparency on the logic of the processing and how it can affect individual rights.

(3) Data Minimization

Data minimization is a basic requirement of privacy protection and has become more urgent as companies collect data they fail to collect. Therefore, NTIA's best practice guides should emphasize the minimization of personal data collection. Companies should only collect data that is absolutely required for a specific purpose or functionality, and promptly dispose of it afterwards. Limiting data collection and retention periods would minimize the potential harm that could result from a hacking incident or a data breach. This approach would minimize the risks to consumers and place privacy responsibilities on companies who collect consumer data.

Conclusion

Privacy protection is critical to continued growth of the Internet, the protection of democratic institutions, and the free flow of information. The NTIA must move quickly to update US privacy law. Voluntary guidelines will do little to solve the very real problems of identity theft, financial fraud, and the ongoing attacks of foreign adversaries on the personal data held by US companies.

[64] § 208 of the E-Government Act (2002), United States Federal Law.

Sincerely,

/s/ Marc Rotenberg
EPIC President

/s/ Sunny Kang
EPIC International Consumer Counsel

/s/ Eleni Kyriakides
EPIC International Counsel

/s/ Christine Bannan
EPIC Administrative Law and Policy Fellow