

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

U.S. CUSTOMS AND BORDER PROTECTION of the

DEPARTMENT OF HOMELAND SECURITY

Announcing the Re-Opening of the Public Comment Period for 21st Century Customs Framework

[Docket No. USCBP–2018–0045]

April 11, 2019

By notice published March 12, 2019, U.S. Customs and Border Protection (“CBP”) reopened the comment period for the 21st Century Customs Framework.¹ The CBP anticipates the development of a vast new network of board control systems that will make automated, and oftentimes opaque, decisions concerning individuals.

EPIC submits these comments to CBP to recommend the adoption of the principles contained in the Universal Guidelines for Artificial Intelligence, endorsed by over 300 organizations and experts.² In particular, EPIC highlights the need for transparency, assessment, and accountability for the 21st Century Customs Framework through publication of methods and factors used by the agency in an algorithmic assessment. Additionally, EPIC demands the system

¹ *Announcing the Re-Opening of the Public Comment Period for 21st Century Customs Framework*, 84 Fed. Reg. 8884, (Mar. 12, 2019), available at <https://www.govinfo.gov/content/pkg/FR-2019-03-12/pdf/2019-04433.pdf>.

² The Public Voice, *Universal Guidelines for Artificial Intelligence* (Oct. 23, 2018) available at <https://thepublicvoice.org/ai-universal-guidelines/> [hereinafter UGAI].

operate fairly and that all decisions affecting individuals involve an opportunity for meaningful human intervention. Finally, the agency should ensure data quality, as well as accuracy, reliability and validity.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy issues.³ EPIC routinely comments on CBP and other Department of Homeland Security data collections and data systems.⁴ EPIC previously submitted comments to CBP urging transparency regarding the algorithms and factors used by the Automated Targeting System’s risk assessments.⁵

I. CBP’s 21st Century Customs Framework will profile individuals using personally identifiable information.

CBP runs algorithms on databases to screen travelers and cargo entering and exiting the country. Several of these data systems combine data from many sources to create profiles or risk assessments on individuals or cargo. Since these systems are often used for screening of both individuals and cargo, even the systems used for cargo contain personally identifiable information (“PII”). Much of how these systems operate remains opaque, including the factors and methods used for screening. Although CBP claims that risk scores are only used on cargo and not individuals, PII is used, and the impact of cargo being withheld or pulled for additional screening falls on individuals.

³ EPIC, *About EPIC* (2019), <https://epic.org/epic/about.html>.

⁴ EPIC, *et. al.*, Comments on Notice of Privacy Act System of Records, U.S. Dep’t of Homeland Sec., Docket No. DHS-2006-0060 (2006), <https://www.epic.org/apa/comments/EPIC-ATS-Comments-2006.pdf>; EPIC, Comments on Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-024 CBP Intelligence Records System (CIRS) System of Records, U.S. Customs and Border Prot., U.S. Dep’t of Homeland Sec., Docket No. DHS-2017-0027; 2017-0027 (Oct. 23, 2017), available at <https://www.epic.org/apa/comments/EPIC-CBP-Intelligence-Records-System-Comments.pdf>.

⁵ EPIC, Comments on the Automated Targeting System Notice of Privacy Act System of Records and Proposed Rule: Privacy Act of 1974 Exemptions, U.S Customs and Border Protection, U.S. Dep’t of Homeland Sec., Docket Nos. 2012-0019; 2012-0020 (June 21, 2012), available at <https://epic.org/privacy/travel/ats/EPIC-ATS-Comments-2012.pdf>.

a. *Automated Targeting System*

CBP's Automated Targeting System ("ATS") "compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments."⁶ ATS creates rules by comparing information about "cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP Officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence."⁷ ATS may flag a person, shipment, or conveyance, even without any association with a previous law enforcement action or other note of law enforcement concern, using "predictive analytics."⁸ "ATS uses data from many different source systems. In some instances ATS is the official record for the information, while in other instances ATS ingests and maintains the information as a copy or provides a pointer to the information in the underlying system."⁹ ATS pulls information from at least 25 government databases, as well as from commercial data aggregators and other manually processed data.¹⁰ Many of these databases contain personally identifiable information.¹¹

ATS makes determinations about individuals and cargo by:

standardiz[ing] names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data and personal information to form a more complete picture of a traveler, import, or export in context with previous behavior of the parties involved. Traveler, conveyance, and

⁶ U.S. Customs and Border Prot., U.S. Dep't of Homeland Sec., DHS/CBP/PIA-006(e), Privacy Impact Assessment Update for the Automated Targeting System, 1 (Jan. 13, 2017), available at <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006-ats-december2018.pdf> [hereinafter ATS PIA].

⁷ ATS PIA, 1.

⁸ ATS PIA, 4; U.S. Dep't of Homeland Sec., *2017 DHS Data Mining Report to Congress*, 10 (Oct. 2018), available at https://www.dhs.gov/sites/default/files/publications/2017-dataminingreport_0.pdf [hereinafter Data Mining Report].

⁹ ATS PIA, 2.

¹⁰ ATS PIA, 82-83.

¹¹ ATS PIA, 82-83.

shipment data are processed through ATS and are subject to a real-time, rules-based evaluation.¹²

The system uses “data mining, machine learning, and other analytic techniques to enhance [its cargo screening modules].”¹³ Because PII is used to make decisions that impact individuals, it is imperative that the methods—now mostly secret—and factors used in making targeting assessments are made public, and that the system is governed by ethics and accountability.

b. Analytical Framework for Intelligence

CBP uses the Analytical Framework for Intelligence (“AFI”) “to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS at the border.”¹⁴ AFI serves as a single access point for analysis and development of intelligence products and incorporates records from at least 9 other CBP and DHS systems, many of which include PII.¹⁵

CBP uses AFI to “gather and develop information about persons, events, and cargo or conveyances of interest by creating an index of the relevant data in the existing operational systems, and providing certain AFI users with different tools that assist in identifying non-obvious relationships.” The methods of identifying “non-obvious relationships” are largely unexplained.¹⁶ Since automated analysis is used to discover “non-obvious relationships,” there is a strong need for regulations to prevent discrimination or other unfair impacts on individuals.

c. CBP Intelligence Records System

CBP’s Intelligence Records System (“CIRS”) allows the agency to “collect and consolidate information from multiple sources” to “[i]dentify, apprehend, or prosecute

¹² Data Mining Report, 13.

¹³ Data Mining Report, 16.

¹⁴ U.S. Customs and Border Prot., U.S. Dep’t of Homeland Sec., DHS/CBP/PIA-010(a), Privacy Impact Assessment Update for the Analytical Framework for Intelligence (AFI), 1 (Sept. 1, 2016), available at <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-afi-march2019.pdf> [hereinafter AFI PIA].

¹⁵ AFI PIA, 1, 3.

¹⁶ Data Mining Report, 30.

individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. border security.”¹⁷ As EPIC previously commented, the categories of records in this database are virtually unlimited and implicates individuals who are not under investigation.¹⁸ This data includes PII in the form of biographic information, immigration information, law enforcement information, and even news articles or social media information.¹⁹ The use of leads for investigation gleaned from social media or traditional news media is particularly alarming, since these assumptions cannot easily be verified. This further emphasizes the need for monitoring and transparency of the use of AI in these systems.

II. CBP should adopt the Universal Guidelines for Artificial Intelligence.

The 21st Century Customs Framework should include a commitment to the principles, rights, and obligations contained in the Universal Guidelines for Artificial Intelligence. CBP's framework, which uses machine learning and algorithms to make decisions that impact individuals, should be governed by clear policy rules set out in agency regulations. There are

¹⁷ Privacy Act of 1974; DHS/CBP–024 Intelligence Records System (CIRS) System of Records, 82 Fed. Reg. 44198, 44200 (Sept. 21, 2017), available at <https://www.federalregister.gov/documents/2017/09/21/2017-19718/privacy-act-of-1974-dhscbp-024-intelligence-records-system-cirs-system-of-records> [hereinafter CIRS SORN].

¹⁸ EPIC, Comments on the Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-024 CBP Intelligence Records System (CIRS) System of Records, U.S. Customs and Border Protection, U.S. Dep’t of Homeland Sec., Docket No. DHS-2017-0026 and 0027, 4, 8 (Oct. 23, 2017), available at <https://epic.org/apa/comments/EPIC-CBP-Intelligence-Records-System-Comments.pdf>; 82 Fed. Reg. 44200-01.

¹⁹ 82 Fed. Reg. 44200.

several guidelines in the UGAI that are particularly applicable to CBP's 21st Century Customs Framework.

a. Right to Transparency and the Assessment and Accountability Obligation

Although the 21st Century Customs Framework applies to trade, trade is at root between individuals, and individuals and their rights will be impacted by the decisions made by the systems of the Framework. Therefore, the Universal Guidelines for Artificial Intelligence apply to the Framework and its use of analytical and machine learning algorithms.

The principle of transparency is found in various modern privacy laws including the US Privacy Act, the EU Data Protection Directive, the GDPR, and the Council of Europe Convention 108. The aim of transparency is to “enable independent accountability for automated decisions.”²⁰ This principle translates into an affirmative right of individuals, “to know the basis of an AI decision that concerns them[,]” including “access to the factors, the logic, and techniques that produced the outcome.”²¹ Individuals should not be left in the dark about analytical systems making decisions that affect them.

Further, CBP should implement an assessment and accountability mechanism. The UGAI states that “An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system.”²² There is no indication that a full assessment and proper accountability

²⁰ The Public Voice, *Universal Guidelines for Artificial Intelligence Explanatory Memorandum and References* (Oct. 2018), available at <https://thepublicvoice.org/ai-universal-guidelines/memo/> [hereinafter UGAI Explanatory Memo].

²¹ UGAI, 1.

²² UGAI, 5.

mechanisms are in place for the various systems that will make up the 21st Century Customs Framework, including the ATS, AFI, and CIRS.

EPIC urges CBP to create and publish “Algorithmic Assessments” similar to the Privacy Impact Assessments conducted by federal agencies pursuant to Section 208 of the E-Government Act of 2002. These assessments would force the agency to determine the risks of an AI system prior to deployment. The assessments would also allow individuals to understand the methods and factors used in decisions that have an impact on their lives.

b. Fairness Obligation and Right to Human Determination

As the Universal Guidelines state, “Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions.” This fairness obligation is particularly important to ensure that the systems of the Framework are not used to make decisions that will adversely affect particular groups for illegitimate reasons. It is important to remember that seemingly neutral factors and rules could lead to impermissible discriminatory results.²³ As such, even in the customs context, it is important to ensure that proper care is taken to ensure fairness.

This is particularly true for CBP, since some of its systems, such as the Automated Targeting System, use “information that could directly indicate the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life” of individuals.²⁴ It is unclear how this data relates to screening cargo, and even if it did, the

²³ Joi Ito, *Supposedly 'Fair' Algorithms Can Perpetuate Discrimination*, Wired (Feb. 5, 2019), <https://www.wired.com/story/ideas-joi-ito-insurance-algorithms/>.

²⁴ EPIC, Comments on the Automated Targeting System Notice of Privacy Act System of Records and Proposed Rule: Privacy Act of 1974 Exemptions, U.S Customs and Border Protection, U.S. Dep’t of Homeland Sec., Docket Nos. 2012-0019; 2012-0020, 1 (June 21, 2012), available at <https://epic.org/privacy/travel/ats/EPIC-ATS-Comments-2012.pdf>.

potential for abuse and unfair results is strong. The utility of big data is alluring, but it is important to avoid perpetuating unfair bias or discrimination by way of automation.

The right to meaningful human intervention is helpful to ensure algorithmic discrimination does not take place. Human decisionmaking “reaffirms that individuals and not machines are responsible for automated decision-making.”²⁵ With better accountability for the results of such systems, there is less of a chance of unfair results.

c. Accuracy, Reliability, and Validity Obligations and Data Quality Obligation

The obligations of accuracy, reliability, validity, and data quality are important principles in any system, especially in one intended to protect against illegal trade. These obligations are all the more important for CBP to commit to since the agency has exempted the underlying systems of the Framework, including the AFI and CIRS, from Privacy Act obligations that require the information in these system to be relevant and necessary.²⁶ Indeed, the agency attempts to justify these exemptions from the Privacy Act by acknowledging that the information collected in these systems is not always accurate.²⁷ Therefore, CBP must verify the information used in the systems included in the Framework and should frequently audit such systems.

III. Conclusion

CBP should adopt Universal Guidelines for Artificial Intelligence. In particular, the agency should produce and publish “Algorithmic Assessments” to ensure transparency and

²⁵ UGAI Memo.

²⁶ See, e.g., *Final Rule, Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security U.S. Customs and Border Protection, DHS/CBP—017 Analytical Framework for Intelligence (AFI) System of Records*, 77 Fed. Reg. 47767 (Aug. 10, 2012); *Final Rule, Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)—024 CBP Intelligence Records System (CIRS) System of Records*, 83 Fed. Reg. 66557 (Dec. 27, 2018).

²⁷ *Id.*

accountability, ensure that the systems are not impermissibly discriminatory, and vigilantly audit data quality.

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott

Jeramie D. Scott
EPIC Senior Counsel

/s/ Ellen Coogan

Ellen Coogan
EPIC Domestic Surveillance Fellow