epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Department of Justice

In re Criminal Justice Chatbot Market Survey

87 Fed. Reg. 9,643

April 8, 2022

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Department of Justice's ("DOJ") Request for Information regarding its Criminal Justice Chatbot Market Survey ("Chatbot Survey").[1]

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues and to protect privacy, the First Amendment, and constitutional values.

EPIC has litigated for the disclosure of documents regarding "evidence-based risk assessment tools,"[2] has uncovered substantial information about risk assessment tools used in state and local agencies around the U.S.[3], and routinely urges government actors to act quickly to regulate the use of artificial intelligence and automated decision-making technologies, particularly when applied in sensitive contexts.[4]

---

[1] Criminal Justice Chatbot Market Surve, Justice Programs Office, 87 FR 9643 https://www.federalregister.gov/documents/2022/02/22/2022-03620/criminal-justice-chatbot-market-survey
[2] EPIC, *EPIC v. DOJ (Criminal Justice Algorithms)* https://epic.org/foia/doj/criminal-justice-algorithms/.
[3] EPIC, *Liberty at Risk*
[4] *See* EPIC,Comments to the Office of Management and Budget, *Request for Comments on a Draft Memorandum to the Heads of Executive Departments and Agencies, "Guidance for Regulation of Artificial Intelligence*

EPIC advocates for the adoption of the Universal Guidelines for Artificial Intelligence, a framework for AI governance based on the protection of human rights set out at the 2018 Public Voice meeting in Brussels, Belgium.[5] The Universal Guidelines for AI have been endorsed by more than 250 experts and 60 organizations in 40 countries.[6] The UGAI comprise twelve principles:

1. Right to Transparency.
2. Right to Human Determination.
3. Identification Obligation.
4. Fairness Obligation.
5. Assessment and Accountability Obligation.
6. Accuracy, Reliability, and Validity Obligations.
7. Data Quality Obligation.
8. Public Safety Obligation.
9. Cybersecurity Obligation.
10. Prohibition on Secret Profiling.
11. Prohibition on Unitary Scoring.
12. Termination Obligation.[7]

Among other key principles, the UGAI states: "All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome" (*Right to Transparency*); "Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions" (*Fairness Obligation*); "An AI system should be used 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" (*Assessment and Accountability Obligation*); "Institutions must ensure the accuracy, reliability, and validity of decisions" (*Accuracy, Reliability, and Validity Obligations*); and "Institutions must establish data provenance and assure quality and relevance for the data input into

Applications," 85 Fed. Reg. 1825, Office of Management and Budget (Mar. 13, 2020); EPIC, Comments to the National Security Commission on Artificial Intelligence, 85 Fed. Reg. 32,055 (Sep. 30, 2020) https://epic.org/wp-content/uploads/apa/comments/EPIC-comments-to-NSCAI-093020.pdf

[5] *Universal Guidelines*, *supra* note 16.

[6] *Universal Guidelines for Artificial Intelligence: Endorsement*, The Public Voice (2020), https://thepublicvoice.org/AI-universal-guidelines/endorsement/.

[7] *Universal Guidelines*, *supra* note 16.

algorithms" (*Data Quality Obligation*). Although some chatbots may not be considered "AI," the DOJ can and should still consider these principles when evaluating, recommending, adopting, or issuing guidance with respect to chatbots.

The DOJ should carefully consider whether grant programs for chatbots throughout the criminal justice system are appropriate and should not recommend, adopt, or facilitate the use of chatbots absent robust data governance rules and transparency requirements.

Regardless of whether the DOJ ultimately facilitates grant programs for chatbot adoption, DOJ's market survey will reflect the values of the agency and communicate accepted standards. In these comments, EPIC recommends that the DOJ investigate and highlight chatbot products that focus on and uphold strict data collection, minimization, and use policies.. EPIC also urges the DOJ to investigate and highlight the limited utility of chatbots, the potential dangers of overreliance, and the collateral consequences of widespread adoption.

I. The Department of Justice Should focus on and establish strict requirements regarding data collection, minimization, and use.

The DOJ developed a strong framework for thinking about use of chatbots in its National Institute for Justice Report, *Chatbots in the Criminal Justice System*.[8] Implementing the findings of that report, however, requires more than a simple checklist of questions to ask.[9] The DOJ should develop and implement strict requirements to minimize the use of chatbots in the criminal justice system, protect privacy, and ensure the safety of individuals using chatbots. A simple set of rules enforced by regular audits would go a long way toward mitigating the potential harms to individuals interacting with automated messaging systems, which are particularly significant in the context of the justice system.

---

[8] Steven Schuetz, Jeri D. Ropero-Miller, & Jim Redden, Chatbots in the Criminal Justice System, National Institute for Justice (Oct. 2021), https://cjtec.org/files/chatbots-criminal-justice (*hereinafter* NIJ Chatbot Report)..

[9] *Id*. at 14, while a checklist may be helpful for identifying risks from a chatbot, simply requiring consideration of risks is not enough to prevent the use of harmful systems.

The NIJ Chatbot Report helpfully identifies four main categories of chatbots in the justice system: Law Enforcement Recruitment and Investigations, Court System Awareness and Access, Corrections and Community Supervision, and Victim Services and Support.[10] With respect to chatbots that provide information to individuals interacting with the justice system and those that provide basic "check in" monitoring services, the following rules should be implemented:

- Data Collection: a chatbot should only collect the data necessary to provide the user with the service it is designed to provide;
- Data Retention: a chatbot should only retain personal information for the span of time required to provide the service;
- Use Limitation: information disclosed to chatbots or inferences drawn from that information should only be used for the express purpose the chatbot is designed to provide;
- Auditing: each chatbot should be regularly audited for (1) effectiveness and (2) compliance with privacy safeguards.

These recommended rules dovetail with the Department of Homeland Security's Fair Information Practice Principles (FIPPs), providing a strong rubric for evaluating chatbot systems.[11] The FIPPs include Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.

The National Institute for Justice recognizes that "chatbots should collect as little personal information as possible."[12] Restricting data collection is necessary to prevent abuses of chatbot systems and reduce the risk of mission creep for agencies administering chatbots. Individuals interacting with chatbots designed to provide information, support, or community supervision will

[10] *Id*. at 4.
[11] Hugo Teufel III, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, *Mem.No. 2008-01*, Dept. of Homeland Sec. (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.
[12] *Id*. at 10.

often be in vulnerable positions.[13] Strict data retention policies work in tandem with limits on data collection to prevent wrongful uses of personal data.

Limiting data collection and retention and designing chatbots to protect vulnerable individuals can prevent harm. For example, domestic violence experts recommend that websites providing resources to victims provide "quick escape" buttons.[14] For criminal justice chatbots, designers should reject the use of cookies and decline to enable chatbots to recognize repeat visitors by IP address so that victims of domestic violence are not accidentally outed by such systems. Design choices like rejecting cookies and not saving IP addresses comply with data minimization principles by avoiding the collection and retention of data that is not strictly necessary to provide the service.

Use limitation policies are equally necessary to minimize abuse and prevent the government and third-party providers from exploiting personal information disclosed solely to obtain information or a service. Even when chatbot systems clearly disclose how individuals' data will be used, those individuals lack the opportunity for meaningful consent. Court system and victims services chatbots may be the only expedient means for individuals to get information about court rules, the progress of their case, or their legal obligations. A choice between an hours-long wait time to speak to an individual and an instantaneous answer from a chatbot is no choice at all. And individuals using probation/parole chatbots lack any capacity to consent. It is vital to prevent further investigation or exploitation of information disclosed to chatbots and to prevent third-party companies from using or

[13] *See, e.g. Using Chatbot Technology to Improve how Law Enforcement Responds to Victims of Residential Burglary*, RTI International (*last accessed* Apr 8., 2022), https://www.rti.org/impact/chatbots-for-law-enforcement; Rachel Metz, *How chatbots are being used to train crisis counselors*, CNN (Dec. 7, 2021) https://www.cnn.com/2021/12/07/tech/trevor-project-ai-trains-crisis-counselors/index.html

[14] *See*, Exit From This Website Quickly, Tech Safety (*last accessed* Apr. 7, 2022), https://www.techsafety.org/exit-from-this-website-quickly.

selling personal data. These safeguards are necessary to preserve confidence in chatbot systems and prevent harms to individuals.

The recent revelation that the Crisis Text Line was exploiting user data to develop an algorithm for a for-profit company illustrates why use limitation is necessary to maintain trust in chatbot systems and keep these systems accessible and useful. Crisis Text Line is a suicide hotline texting service that amassed a large volume of data from individuals reaching out for support and responding to automated prompts in a chatbot-like feature.[15] The non-profit then licensed "anonymized" data derived from its chatbot to a for-profit company, which in turn was building a service to counsel customer service representatives on de-escalation techniques.

The DOJ should be careful to evaluate products in the criminal justice system for similar risks and, where the possibility of data abuse exists, to minimize that risk by rigorously enforcing use limitation policies. The DOJ should also be particularly careful about developing chatbot systems for use in the criminal justice system with vendors that sell other products and services that it might try to build or enhance with chatbot data, as there is a heightened risk that the vendor will misuse sensitive personal data collected through its chatbot products.

The Department should not endorse or provide funds to support the use of chatbots for investigative purposes. The NIJ Chatbot Report notes that in "New York, Los Angeles, Chicago, and Boston, law enforcement agencies have used chatbots in 'stings' in which the chatbots pose as minors offering commercial sex services as a campaign to identify buyers and combat sex trafficking."[16] Individuals interacting with these chatbots have no opportunity to provide consent and are unaware that they are interacting with an algorithm. Chatbots may magnify the risks of

[15] Keith Porcaro, *The Real Harm of Crisis Text Line's Data Sharing*, Wired (Feb. 1, 2022), https://www.wired.com/story/consumer-protections-data-services-care/; Jasmine Hicks and Richard Lawler, *Crisis Text Line stops sharing conversation data with AI company*, The Verge (Feb. 1, 2022), https://www.theverge.com/2022/1/31/22906979/crisis-text-line-loris-ai-epic-privacy-mental-health.
[16] NIJ Chatbot Report at 4.

entrapment inherent in undercover operations by optimizing conversations to induce illegal activities. Given the risks to privacy and civil liberties, the DOJ should simply opt not to pursue or support the use of chatbots for investigative purposes.

II. The Department of Justice Should Require Transparency and Robust Oversight Mechanisms for Chatbot Products.

The DOJ should not recommend, highlight, or allow grant funds to be spent on chatbots from companies that withhold vital information about their systems by invoking protections for trade secrets or other commercial information.

Many government contractors, even in the criminal justice system, often agree only to contracts that require the agency using their products to protect their commercial interests.[17] Other contracts related to criminal justice not proactively disclosed in procurement registries.[18] The DOJ should make clear that the logic and data practices of a chatbot used by the DOJ or funded through a DOJ grant must not be withheld from the public under the guise of trade secrets.

Chatbots used in the criminal justice system handle extremely sensitive data and may have a significant impact on individuals' livelihoods and liberty. In addition to being a vector for the misuse of sensitive information, these systems often interact with people at their most vulnerable moments.[19] As such, the DOJ must evaluate and hold these contractors to a high standard of data and civil rights protection.

---

[17] EPIC Amicus Brief, *Citizens for Responsibility and Ethics in Washington (CREW) v. Department of Justice, D.C. Circuit* No. 21-5276, available at https://epic.org/documents/citizens-for-responsibility-and-ethics-in-washington-crew-v-department-of-justice/

[18] EPIC Liberty at Risk report, supra 2

[19] *See generally* Todd Feathers, *Payday Lenders are Big Winners in Utah's Chatroom Justice Program*, MarkUp (Mar 16, 2022) https://themarkup.org/remote-justice/2022/03/16/payday-lenders-are-big-winners-in-utahs-chatroom-justice-program;; Bob Ambrogi, *How We Rapidly Iterated A Chatbot to Track Probationers During the Pandemic*, Lawsites (Apr 21, 2020) https://www.lawnext.com/2020/04/guest-post-how-we-rapidly-iterated-a-chatbot-to-track-probationers-during-the-pandemic.html

The DOJ should create a replicable regime of transparency, audits, impact assessments, approval, licensure, registration, and recertification to maximize accountability. The agency should also require that any system can produce clear documentation of data collection, use, and lifecycle.

Transparency of what system a given government agency is using, along with understandable decision-tree logic of how the system works and data collection, use, sharing, and retention policies should be an absolute bare minimum requirement for any chatbot product that the DOJ highlights or analyzes. . These requirements hcan require collaboration between the agency and the vendor, but the onus to ensure transparency should remain on the agency.

Both audits and impact assessments can help improve the accountability of systems—like chatbots—that collect and process personal information. But an audit or impact assessment that lacks *sufficient consequences or enforcement* can turn into a meaningless box-checking exercise. EPIC recommends the DOJ use the following resources to guide development of its algorithmic impact assessment procedures:

- Kate Crawford, Dillon Reisman, Jason Schultz, & Meredith Whittaker, Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability, AI Now Institute (2018),
- Jacob Metcalf, Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh, & Madeleine Clare Elish, Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts, FAccT (Mar. 3, 2021),
- Ada Lovelace Institute, AI Now Institute, & Open Government Partnership, Algorithmic Accountability for the Public Sector (2021)

Independence and transparency are key to any of these oversight mechanisms, and it is critical to impose meaningful consequences for noncompliance.

III. Conclusion

EPIC recommends that the DOJ's market survey on chatbots in the criminal justice system focus on use specification and limitations; data collection, retention, use, and sharing policies among others. EPIC also urges the DOJ to carefully consider where the use of chatbots in the criminal

justice system is appropriate, and establish robust oversight that is transparent and improves accountability

Respectfully,

/s/ *Ben Winters*
Ben Winters
EPIC Counsel

/s/ *Jake Wiener*
Jake Wiener
EPIC Law Fellow