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

Office of the Privacy Commissioner of Canada

Notice of consultation and call for comments: Privacy guidance on facial recognition for police agencies

October 15, 2021

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the Office of the Privacy Commissioner of Canada's ("OPC's") notice of consultation and call for comments regarding the draft privacy guidance on facial recognition for police agencies (hereinafter, "Draft Guidance").[1] The OPC seeks input on the Draft Guidance in the form of responses to specific questions posed in the call for comments.[2]

EPIC urges the OPC to consider the serious risks to privacy and human rights inherent in facial recognition technology and whether issuing guidance on its use confers tacit approval or endorsement of the technology. The Draft Guidance specifically notes several unmitigated risks yet falls short of advocating a ban on use of facial recognition. EPIC recommends that the OPC commit to fully banning use of facial recognition technology and until that time, make a statement that use of the technology is by its nature an impingement on privacy and human rights. Further, EPIC recommends more specific examples and recommendations within the Draft Guidance to impose more meaningful limitations on facial recognition technology and curb overbroad and discretionary

[1] Office of the Privacy Commissioner of Canada, *Notice of consultation and call for comments – Privacy guidance on facial recognition for police agencies*, available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/notice_frt/.
[2] *Id.*

use. As it stands, the Draft Guidance is more likely to whitewash abusive surveillance practices than to provide meaningful privacy protections.

EPIC is a public interest research center in Washington, D.C., 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 a long history of pushing for a ban on the use of facial recognition technology and for clear limitations, transparency, and accountability in its use.[3] EPIC has successfully lobbied for an end to DC-area facial recognition system use and submitted FOIA requests relating to federally-funded fusion center use of facial recognition systems on protestors.[4]

[3] *See, e.g.,* Ban Face Surveillance, EPIC Campaign, details available at https://epic.org/banfacesurveillance/; Testimony of EPIC, Massachusetts Joint Committee on the Judiciary (Oct. 22, 2019), https//epic.org/testimony/congress/EPIC-FacialRecognitionMoratorium-MA-Oct2019.pdf; EPIC, *Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology*, Coalition Letter (June 3, 2021), https://epic.org/privacy/facerecognition/Civil-Rights-Statement-of-Concerns-LE-Use-of-FRT-2021.pdf; EPIC, *Letter to President Biden on Implementing a Facial Recognition Technology Moratorium*, Coalition Letter (Feb. 16, 2021), https://epic.org/privacy/facerecognition/Coalition-Letter-Biden-FRT-Moratorium.pdf.

[4] Response Letter to EPIC, *Response to letter on the National Capital Region Facial Recognition Investigative Leads System*, Metropolitan Washington Council of Governments (May 14, 2021), https://epic.org/privacy/facerecognition/MWCOG-Letter-Ending-NCRFRILS.pdf; EPIC, *Right to Know Law Request*, Pennsylvania Fusion Centers (March 17, 2021), https://epic.org/foia/fusioncenter/EPIC-2021-03-17-DVIC-FOIA-20210317-Request.pdf; EPIC, *S.C. Freedom of Information Act Request,* South Carolina Fusion Centers (March 17, 2021), https://epic.org/foia/fusioncenter/EPIC-2021-03-17-SCIIC-FOIA-20210317-Request.pdf; EPIC, *California Public Records Act Request*, California Fusion Centers (March 17, 2021), https://epic.org/foia/fusioncenter/EPIC-2021-03-17-NCRIC-FOIA-20210317-Request.pdf; EPIC, *Open Records Law Request,* North Dakota Fusion Centers (March 17, 2021), https://epic.org/foia/fusioncenter/EPIC-2021-03-17-NDSLIC-FOIA-20210317-Request.pdf.

EPIC's response to OPC's Call for Comments.

1. **Will this guidance have the intended effect of helping to ensure police agencies' use of FR is lawful and appropriately mitigates privacy risks? If you don't believe it will, why?**

Despite the thoughtfulness behind the Draft Guidance and the attempt to address the high risks of facial recognition, EPIC does not believe that the Draft Guidance is sufficient to ensure lawful use of facial recognition and appropriately mitigate the privacy risks.

Lawfulness of facial recognition will fluctuate, and lawfulness does not preempt ethics.

When it comes to lawfulness of facial recognition use, there are two factors to our concerns. First, even if facial recognition use is lawful (or at least not specifically unlawful) in certain areas or contexts, that does not mean that it will continue to be lawful. The "patchwork of statutes and case law"[5] tied to facial recognition, including the Quebec biometric privacy regulation cited within the Draft Guidance,[6] makes creating a universally applicable guidance framework nearly impossible.[7] At the very least, any guidance attempting to address facial recognition use must be capable of evolving swiftly along with ever-changing regulations. EPIC is not confident that the current Draft Guidance is agile enough to do so in such a way that will still provide meaningful and specific guidance to police agencies. The second concern with lawfulness is whether legality is the key question—indeed,

[5] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Introduction (14).
[6] *See* Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Introduction (36).
[7] Based on the proliferation of new biometric and facial recognition bans globally, the shifting regulatory status shows no signs of settling; *see, e.g.*, Shannon Flynn, *13 Cities Where Police Are Banned From Using Facial Recognition Tech*, Innovation & Tech Today (Nov. 18th, 2020), https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/; Dave Gershgorn, *Maine passes the strongest facial recognition ban yet*, The Verge (June 30, 3031), https://www.theverge.com/2021/6/30/22557516/maine-facial-recognition-ban-state-law; Julie Carr Smyth, *States push back against use of facial recognition by police*, ABC News (May 5, 2021), https://abcnews.go.com/Politics/wireStory/states-push-back-facial-recognition-police-77510175; Paul Bischoff, *Facial recognition technology (FRT): 100 countries analyzed*, Comparitech (June 8, 2021), https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/ (noting that Belgium and Luxembourg have both banned facial recognition technology).

a practice may be legal and also harmful or unethical. This leads us to the question of appropriately mitigating harmful privacy risks—specifically, whether it is possible to meaningfully mitigate privacy risks.

Facial recognition use should be banned entirely.

The Draft Guidance does not appropriately mitigate privacy risks because appropriate mitigation of such a high-risk technology is not possible. Facial recognition cannot be used in a manner that is compatible with privacy and human rights. Indeed, the Draft Guidance itself states that "the freedom to live and develop free from surveillance is a fundamental human right."[8] The Draft Guidance also notes that facial recognition is a "powerful technology that can pose serious risks to privacy."[9] It stands to reason that the use of a powerful surveillance technology with serious privacy risks is incompatible with the fundamental human right acknowledged in the Draft Guidance.

The flaws and risks inherent in facial recognition have been documented extensively, from ending anonymity to delivering incorrect results to proliferating bias and systemic oppression to endangering activists, protestors, and marginalized groups.[10] The imminent threat that facial recognition poses to privacy, civil liberty, and broader human rights has prompted outright bans of

[8] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Introduction (9).

[9] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Overview (1).

[10] *See e.g.* Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, New York Times (Jan. 18, 2020, updated March 18, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; Claudia Garcia-Rojas, *The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies*, Truthout (Mar. 3, 2016), https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police (Discussing Professor Simone Brown's research on how race and anti-Black colonial logics inform contemporary surveillance practices); James Vincent, *The Invention of AI 'Gaydar' Could be the Start of Something Much Worse*, The Verge (Sept. 21, 2017), https://www.theverge.com/2017/9/21/16332760/ai-sexuality-gaydar-photo-physiognomy; *Facial Recognition to "Predict Bias" Sparks Row Over AI Bias,* BBC News (June 24, 2020), https://www.bbc.com/news/technology-53165286; Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of the 1st Conference on Fairness, Accountability, and Transparency, PMLR 81:77-91, 2018.

the technology in several regions.[11] Outside of regulatory efforts, privacy and civil liberty organizations have mobilized multiple campaigns to ban facial recognition.[12] Several of these movements to ban facial recognition rely on the argument made within the Draft Guidance: that the freedom to live free from surveillance is a human right.[13]

Another concern regards the reasonable expectation of privacy. A reasonable expectation of privacy (or “REP”) depends on the level of privacy individuals expect in a free and open society, including what may be observed or captured, how it will be used, and how it will be shared. While courts may vary to some degree on what constitutes a reasonable privacy expectation when it comes to facial recognition, it is clear that facial recognition captures biometric personal data that cannot be changed, that it does so with the ability to identify individuals and tie them to sensitive information, and that its use goes far beyond standard observation by human eyes. Therefore, as the Draft Guidance states, facial recognition “will generally raise a [reasonable expectation of privacy], whether online or in person, despite faces being publicly visible. Individuals do not expect to be the subject of surveillance when going about their normal and lawful activities, and generally maintain some degree of a [reasonable expectation of privacy] even when in public spaces.”[14]

[11] Shannon Flynn, *13 Cities Where Police Are Banned From Using Facial Recognition Tech*, Innovation & Tech Today (Nov. 18th, 2020), https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/; Dave Gershgorn, *Maine passes the strongest facial recognition ban yet*, The Verge (June 30, 3031), https://www.theverge.com/2021/6/30/22557516/maine-facial-recognition-ban-state-law; Julie Carr Smyth, *States push back against use of facial recognition by police*, ABC News (May 5, 2021), https://abcnews.go.com/Politics/wireStory/states-push-back-facial-recognition-police-77510175; Paul Bischoff, *Facial recognition technology (FRT): 100 countries analyzed*, Comparitech (June 8, 2021), https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/ (noting that Belgium and Luxembourg have both banned facial recognition technology).

[12] *See e.g.* “Ban Facial Recognition,” https://www.banfacialrecognition.com/; Angela Chen, *40 groups have called for a US moratorium on facial recognition technology*, Technology Review (Jan. 27, 2020), https://www.technologyreview.com/2020/01/27/276067/facial-recognition-clearview-ai-epic-privacy-moratorium-surveillance/.

[13] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Introduction (9).

[14] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Lawful Authority: The Charter (53).

Despite the Draft Guidance recognizing the inherent risks of facial recognition use and the conflict between those risks and privacy and human rights, the Draft Guidance stops short of banning facial recognition altogether or even making a clear statement that use of facial recognition technology is not recommended. Instead, the Draft Guidance states that facial recognition may be useful for law enforcement when used "responsibly and in the right circumstances."[15] We fail to see how such use can be possible.

<u>If facial recognition use is not banned, the guidance must be more specific.</u>

If a full ban on facial recognition use is not imposed, the Draft Guidance must be significantly more detailed to mitigate privacy harms. Several of the recommendations include vague missives rather than clear examples of how to implement directives.

For example, the Draft Guidance explicitly identifies the connection between surveillance and systemic discrimination.[16] However, urging law enforcement agencies to "account for and respect the right to equal protection and equal benefit of the law without discrimination" provides no recommendations or assistance in determining how to do so.[17] Acknowledgement of a problem is an excellent step, but law enforcement agencies using high-risk technology cannot be left entirely on their own to solve the problem.

The Draft Guidance later states that there may be cases where "potential harms may be so extreme that no amount of protections can be applied to adequately reduce the privacy risk."[18] Yet the Draft Guidance provides no examples of these extreme potential harms, no case examples, no clear prohibitions on when facial recognition use may be wholly unjustifiable. The lack of specificity

[15] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Introduction (4).
[16] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Introduction (11).
[17] *Id.*
[18] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Privacy Framework (31).

here does not aid law enforcement or protect privacy. It merely allows the Draft Guidance the façade of a hard line on facial recognition use without drawing that hard line.

A lack of specificity may also pave the way for abuse of discretion. For example, the Draft Guidance states that facial recognition objectives must be specific and that agencies using facial recognition should "demonstrate the pressing and substantial nature of the specific object" and ensure that personal information collected is "tailored and necessary" to the specific goal.[19] Leaving it to law enforcement agencies to determine what constitutes a "pressing and substantial" objective or how broad "tailored and necessary" personal information collection may be opens the door for overly broad interpretations, rendering any attempted protections through these measures essentially meaningless. Even the use of specific examples would serve to more firmly bound the limits of what may fall within those descriptions.

Similarly, the recommendation to review data holdings at "regular intervals" with no baseline requirement or guidance allows for abuse (after all, review every ten years would be "regular," but would defeat the intent of the review),[20] as does the mandate that individuals be informed of facial recognition use at the time of collection without any specifics regarding the form, availability, or prominence of the notice.[21] Without specific use mandates, including examples of permitted and not permitted uses, baseline requirements, and clear boundaries, the well-intentioned principles contained in the Draft Guidance will be rendered unable to meaningfully protect privacy and human rights.

[19] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Lawful Authority: Necessity and Proportionality (57).
[20] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Retention (101).
[21] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Openness, transparency and individual access (103).

2. Can this guidance be practically implemented?

Police agencies cannot be trusted to effectively implement limits on facial recognition technology. The mass rollout of law enforcement facial recognition systems ("FRSs") in the last decade occurred without input from civil society or caution on the part of police departments. Both the nature of facial recognition services and the incentive structure for police make meaningful oversight difficult, if not impossible. The Draft Guidance does not adequately address these problems and in particular falls short by leaving police departments to establish their own standards and metrics for privacy-protective behavior.

Police routinely adopt facial recognition systems in secret.

Police agencies worldwide have adopted facial recognition systems without first consulting civil society and receiving approval from the communities they operate in. By failing to subject themselves to public scrutiny before adopting new highly invasive surveillance technologies, police demonstrated that they cannot be trusted with those technologies. As the Privacy Commissioner is well aware, the Royal Canadian Mounted Police ("RCMP") violated Canada's Privacy Act by using Clearview AI's facial recognition product.[22] The RCMP initially lied to reporters about the agency's use of Clearview AI's facial recognition product, and later could not even provide a reason for 85% of searches performed using the system.[23] Toronto Police similarly obfuscated the agency's use of Clearview AI. The agency denied to reporters that officers had used the product for over a month before reversing course and admitting that the agency had been using Clearview.[24] Neither the

[22] Daniel Therrien, Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology, Office of the Privacy Commissioner of Canada (Jun. 10, 2021), https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#toc1.

[23] *Id.*

[24] *Toronto police admit using secretive facial recognition technology Clearview AI*, CBC News (Feb. 13, 2020), https://www.cbc.ca/news/canada/toronto/toronto-police-clearview-ai-1.5462785.

RCMP nor Toronto PD announced their use of facial recognition—instead the agencies sought to keep it secret.

Police agencies around the world similarly hide their use of facial recognition to avoid scrutiny. In the United States, more than 1,800 federal, state, and local agencies have used Clearview AI without meaningful oversight or any public notice.[25] A Buzzfeed investigation found that law enforcement agencies from the massive Immigrations and Customs Enforcement agency to small local police departments had performed hundreds of thousands of searches through Clearview.[26] The story is the same around the globe, with at least 88 law enforcement agencies outside the US using Clearview before February, 2020.[27] Many of those agencies were in the European Union, where the GDPR should have prevented unannounced use of facial recognition systems. In short, police agencies continuously duck oversight and hide their use of a highly controversial facial recognition tool.

Misuse of facial recognition is a systemic problem at police agencies that is not limited to one facial recognition product or one type of agency. It is the modus operandi of modern police to secretly use facial recognition. The same agencies regularly use the technology to monitor protesters and surveil activists. When the U.S. Government Accountability Agency surveyed 42 federal law enforcement agencies, it found that twenty law enforcement branches used some form of facial recognition.[28] The majority of those agencies were completely unable to track employees use of

[25] Ryan Mac, Caroline Haskins, Brianna Sacks and Logan McDonald, *How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations*, Buzzfeed News (Apr. 9, 2021), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition.

[26] *Id.*

[27] Ryan Mac, Caroline Haskins, and Antonio Pequeno IV, *Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here*, Buzzfeed News (Aug. 25, 2021), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.

[28] U.S. Gov't Accountability Office, GAO-21-518, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks (June 3, 2021), https://www.gao.gov/assets/gao-21-518.pdf.

facial recognition systems, making any form of oversight functionally impossible.[29] At least six of those agencies reported using facial recognition to surveil Black Lives Matter protesters in the summer of 2020.[30] Officers with the U.S. Postal Investigation Service, a branch of the U.S. Postal Service, used facial recognition to monitor protesters during the summer of 2020.[31]

Similarly, a coalition of local and federal agencies in Washington, DC secretly established a facial recognition system to search a collection of 1.4 million mugshots assembled from DC-area police departments.[32] That system was used to identify a protester accused of assaulting an officer. The New York Police Department likewise used facial recognition to identify a prominent activist accused of assault due to yelling loudly at a police officer.[33] These are only a few known examples of police using facial recognition systems. The secretive nature of law enforcement investigations and their actions to protect facial recognition systems from public scrutiny make it virtually certain that the technology is heavily used on protesters and other dissidents along with traditionally overpoliced poor and minority communities.

Police are unable to prevent individual officers from using commercial facial recognition products.

Even if higher-ups at police agencies attempt to implement oversight, the nature of the facial recognition marketplace makes meaningful oversight virtually impossible. Clearview AI regularly

[29] *Id*. at 21.
[30] *Id*. at 18.
[31] Jana Winter, *Facial recognition, fake identities and digital surveillance tools: Inside the post office's covert internet operations program*, Yahoo News (May 18, 2021), https://news.yahoo.com/facial-recognition-fake-identities-and-digital-surveillance-tools-inside-the-post-offices-covert-internet-operations-program-214234762.html.
[32] Justin Jouvenal and Spencer S. Hsu, *Facial recognition used to identify Lafayette Square protester accused of assault*, Washington Post (Nov. 2, 2020) https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html.
[33] George Joseph and Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, Gothamist (Aug. 14, 2020), https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.

offers free trial accounts to individual officers to attract sales.[34] These accounts are virtually impossible for agencies to detect or prevent. Numerous other companies also offer off-the-shelf facial recognition products that can be used by a single officer. In one example, an instructor with the Washington National Guard Counterdrug Program managed to secretly obtain a free trial of Clearview and then included information on how to do so in materials for an officer training course.[35] That training continued without challenge until Buzzfeed's investigation publicized the incident and alerted the instructor's agency to his actions.

Police have a strong incentive to avoid meaningful limits on facial recognition.

Facial recognition is a remarkably powerful technology that can power a range of police surveillance activities. Sophisticated facial recognition systems like Clearview AI can deliver not only identities, but whole social media histories up to officers from a single search. In this context, police have a great deal to gain, and little to lose, by maximizing use of facial recognition. The main harms from a police perspective are loss of legitimacy and public outcry. However, those harms will only materialize if use and abuse of facial recognition are revealed and publicized. The track record suggests that agencies can adopt and use facial recognition in the short term without attracting scrutiny. In the heat of an investigation, short term pressures to use facial recognition will likely outweigh potential blowback. Police then are mainly incentivized to use facial recognition and conceal that use.

Communities that learn police are using facial recognition are likely to push back, regardless of how that information is disclosed. A number of municipalities across the United States have banned law enforcement use of facial recognition in recent years after discovering that police were

[34] Ryan Mac, Caroline Haskins, Brianna Sacks and Logan McDonald, *How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations*, Buzzfeed News (Apr. 9, 2021), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition.
[35] *Id.*

using it.[36] Given the broad distrust in police use of facial recognition and the risks involved with any law enforcement use of the technology, police will not avoid public scrutiny by claiming strict compliance with the Draft Guidance but still may use it as a tool to undermine criticism. As the public is unlikely to be able to meaningfully audit compliance, police will be able to claim they are following the guidelines without strictly implementing them. The pressures created by investigations and the lack of meaningful accountability mere guidance provides are unlikely to incentivize strict implementation of the Draft Guidance. However, those same pressures do incentivize using the Draft Guidance as a fig leaf to blunt criticism and hide ongoing abuses.

<u>The Guidance does not set specific standards that can be audited by third parties.</u>

The Guidance will be difficult for departments to meaningfully implement because it lacks strong external standards for police to comply with. Instead, throughout the Guidance, police agencies are instructed to develop their own standards. For example, § 71 of the Guidance leaves police free to define the "regular intervals" for audits and reassessments. Police then could set very long intervals for audits, creating a veneer of legitimacy without catching or preventing harmful practices. Similarly, § 82 does not even suggest numerical thresholds for system accuracy but instead instructs agencies to set their own thresholds for system accuracy. That leaves police free to set low standards that return a large number of matches, facilitating overly broad investigations and increasing the risk of dangerous misidentifications. Agencies are also instructed to set their own data retention limits in §§ 97-101. But the police are not unbiased participants in setting data retention limits, they have a vested interest in retaining as much information as possible, for as long as

[36] *See e.g.* Shannon Flynn, *13 Cities Where Police Are Banned From Using Facial Recognition Tech*, Innovation & Tech Today (Nov. 18th, 2020), https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/; Dave Gershgorn, *Maine passes the strongest facial recognition ban yet*, The Verge (June 30, 3031), https://www.theverge.com/2021/6/30/22557516/maine-facial-recognition-ban-state-law.

possible, to inform future investigations. Police are unlikely to set and stick to short data retention periods that provide meaningful privacy protections.

The Draft Guidance will not be meaningfully implemented both because police departments lack the capability to fully track facial recognition use and because those agencies are unlikely to engage with the Guidance in good faith. The incentive structure for police will likely lead to bare minimum compliance that whitewashes dangerous uses of facial recognition instead of preventing it. Police agencies have had nearly 20 years to adopt facial recognition technology with substantial public input and decision-making. Instead, they have chronically failed to be transparent in their use of facial recognition and regularly use the technology for abusive surveillance practices. The police cannot be trusted with facial recognition.

3. **Are the recommendations in the "accuracy" section sufficient to help ensure police agencies meet their accuracy obligations in FR initiatives?**

The Draft Guidance identifies several issues related to accuracy, both in the “Accuracy” section and throughout the document. The issues raised and accompanying recommendations are a good start but fail to address some key issues.

First, the Draft Guidance states that police agencies “must ensure” that the personal information processed through facial recognition is sufficiently accurate.[37] We are not certain that this requirement can be met without a high level of technical expertise and insight into the specific workings of the facial recognition technology being used. The Draft Guidance previously noted the difficulty in ensuring that images used for matching within facial recognition systems are consistent when it comes to the level of light, orientation, or amount of time that has passed between

[37] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Accuracy (72).

comparison images.[38] Perimeters for quality and accuracy for input images will likely vary according to the facial recognition system used and may be difficult for law enforcement agencies to appropriately filter. In addition, as noted within the Draft Guidance, human review may be insufficient to address issues of accuracy since humans may be overwhelmed by information, be insufficiently trained in moderating content, or be unduly influenced by the facial recognition system—over-relying on the results such that meaningful oversight is lost.[39]

There is also the challenge of the data that the facial recognition may be trained on and biases that may stem from the training data. For example, if a system is trained on mug shots, it may fall prey to the racial bias inherent in the history of policing and the higher rates of arrest and incarceration for people of color.[40] If the law enforcement agencies are developing the facial recognition technologies themselves, they may be able to ensure that the training data is appropriately diverse and high-quality. However, in many cases, agencies will be using comparative databases and technology developed and maintained by third parties. Depending on the third-party used, law enforcement agencies may have limited access to training data or the algorithmic functions of the technology, preventing any meaningful audit and accuracy assurance and entirely preventing a review for bias or discrimination within the system.

[38] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, How does FR Work? (27).

[39] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Accuracy (79).

[40] *See, e.g.*, Clare Garvie, Alvara Bedoya, Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy & Technology (October 18, 2016), available at https://www.perpetuallineup.org/findings/racial-bias; Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, The Atlantic (April 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/; Alex Najibi, *Racial Discrimination in Face Recognition Technology*, Harvard University Blog Special Edition: Science Policy and Social Justice (October 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

Finally, the Draft Guidance permits law enforcement agencies to set the acceptable thresholds for error within facial recognition systems used.[41] This may be another opening for misuse or inconsistency. EPIC recommends that either the Draft Guidance include specific minimum error thresholds for use of facial recognition systems (including at different risk levels, such as ongoing mass surveillance, use for a limited purpose, etc.) or this responsibility be designated to an outside expert party, such as the Privacy Commissioner.

4. Can the recommendations in the guidance concerning the retention and disposal of personal information collected and used during a FR initiative be appropriately operationalized in a law enforcement context? If not, why?

Police agencies are unlikely to adopt and implement retention schedules that adequately protect privacy. As outlined in response to Question 2, police have a strong incentive to maximize data collection and retention for use in future investigations. The Draft Guidance puts the onus on police to determine appropriate data retention schedules and sort facial recognition data into the appropriate categories. It provides no limits on data retention and does not suggest or require outside auditing for compliance with retention schedules. In essence, the Draft Guidance asks the police to check their own excesses without telling them what a robust retention scheme looks like. It is also often unclear whether a particular piece of evidence, including a facial image or facial template, will be relevant to an investigation. Police can then classify virtually any record as potentially relevant and circumvent well-intentioned deletion schedules.

Even where there is a clear mandate to avoid accessing or delete information, police departments have resisted compliance. For example, the NYPD is currently subject to a lawsuit for a pattern of practice of illegally accessing sealed arrest records, contrary to state law.[42] The NYPD

[41] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Accuracy (82).

[42] Nick Pinto, *Secret NYPD Document Teaches Cops to Illegally Raid Sealed Records*, The Intercept (Jul. 21, 2021), https://theintercept.com/2021/07/21/nypd-secret-training-sealed-arrest-records/.

argued that it was in fact technologically unable to segregate or delete sealed arrest records and therefore refused to comply with state law barring access. Without a strong external auditing system, it is virtually impossible to ensure that police actually delete records in a timely manner and prevent illegitimate searches.

5. What measures or practices can police agencies implement to help ensure any third parties involved in FR initiatives operate with lawful authority?

While the information sharing agreements ("ISAs") recommended in the Draft Guidance serve as an excellent step to ensuring that third parties involved in facial recognition use operate with lawful authority, the Draft Guidance falls short of mandating that agreements be in place for all third-party involvement, instead stating that police agencies "should" implement ISAs.[43] EPIC recommends that this be shifted to a more formal mandate, such as clearly stating that facial recognition operations which do not bind involved third parties under appropriate ISAs will be unlawful. In addition, EPIC recommends that the mandate to implement an ISA be extended to include any third-party participation in a facial recognition operation rather than solely operations which explicitly include law enforcement agencies sending relevant information to the third party.

Finally, EPIC recommends that section 91 of the Draft Guidance be modified to state that images sent to third parties in association with facial recognition use may not under any circumstances be added to the third party's face database or used for training (unless the explicit consent of the data subject is obtained by the third party). The current example used in the section is helpful, but a flat ban on use rather than law enforcement taking "reasonable steps" to prevent these actions more fully protects privacy and human rights interests.[44]

[43] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Purpose Limitation (92).
[44] Office of the Privacy Commissioner of Canada, *Draft Privacy Guidance on Facial Recognition for Police Agencies*, Purpose Limitation (91).

Conclusion

EPIC supports the OPC's care and attention to risk in developing the draft guidelines and urges the OPC to carry on this work by modifying language to clearly express that the guidance should not be construed as support for the use of facial recognition technology and that protection of privacy and human rights remains paramount. The OPC must consider an outright ban on facial recognition use and, in the meantime, set specific baseline requirements for use of facial recognition and use clear examples rather than broad recommendations of best practices. The OPC should not proceed with any version of the Draft Guidance that leaves police free to set their own metrics. Such guidance can only serve to cover up further abuses of facial recognition. For more information or any other questions please contact EPIC Global Privacy Counsel Calli Schroeder at schroeder@epic.org or EPIC Fellow Jake Wiener at wiener@epic.org.

Respectfully Submitted,

Calli Schroeder
Calli Schroeder
EPIC Global Privacy Counsel

Jake Wiener
Jake Wiener
EPIC Law Fellow

Jeramie Scott
Jeramie Scott
EPIC Senior Counsel