November 21, 2022

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

*Via electronic filing*

**Re: Access Now's submission to the Federal Trade Commission's request for comments on the prevalence of commercial surveillance and data security practices that harm consumers (*Commercial Surveillance ANPR, R111004)***

## I. Executive summary

Access Now appreciates the opportunity to submit comments to the Federal Trade Commission's ("FTC" or "Commission") request for comments ("RFC") on the prevalence of commercial surveillance and data security practices that harm consumers.[1] The RFC seeks answers to a variety of questions. This submission focuses on the harms stemming from extensive data collection practices, facial recognition, and emotion recognition technology, and data protection principles that would create and enforce adequate safeguards around such activities.

Some of the information presented is already well-known to the FTC. Access Now commends the Commission for the work it has already done to draw attention to and address these harms. Access Now's goal is to highlight data protection principles critical to adopting a human *and* civil rights-centered approach to data privacy and data protection.

Access Now urges the FTC to:

- Define and include a list of binding data protection principles in the law.
- Define the legal basis authorizing companies to process data.
- Include a list of binding individual rights into the law.
- Develop rules that impose limitations on companies' collection, use, and retention of consumer data.
- Protect data security and data integrity.
- Use its full authority to protect individuals against the extensive collection of data and biometric systems.
- Prioritize investigations and meaningful enforcement action of facial recognition vendors when vendors violate privacy, data protection, and other rules through their products' development and use; and

[1] https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

- Take a more critical stance on penalties for companies that mislead consumers on the collection of biometric data by amplifying its use of algorithmic destruction.

## II. Introduction

Access Now provides thought leadership and policy recommendations to the public and private sectors by offering a digital rights perspective to ensure the protection of human rights.[2] Access Now has special consultative status at the United Nations. We also lead the Ban Biometric Surveillance campaign ("BanBS"), which calls for a prohibition on the uses of facial recognition technology ("FRT") and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance. 193 civil society organizations from sixty-three countries worldwide signed the BanBS letter.[3]

Recently, Access Now, Immigrant Defense Project, Just Futures Law, and over thirty-five human rights organizations sent a letter to Amazon Web Services calling on the company to end its agreement to host the United States Department of Homeland Security's (DHS) HART database.[4] As stated in our letter "this mass biometric data collection by DHS is a deep invasion of privacy, an assault on human rights, and places hundreds of millions of people at risk of raids, detentions, deportations, and family separation. By hosting DHS' HART database, AWS is directly facilitating the creation of an invasive biometrics database that will supercharge surveillance and deportation, risking human rights violations."[5]

In Europe, Access Now is part of the Reclaim Your Face campaign, which launched a formal petition to ban biometric mass surveillance in the European Union.[6] We also launched a campaign with All Out, a global LGBT+ organization, to expose the threat of automated gender "recognition" and the use of artificial intelligence ("A.I.") systems to predict sexual orientation.[7] In addition, we facilitate the #WhyID community to ensure that digital identity programs respect the rights of people around the world.[8]

Access Now is pleased to see that the rapid and harmful expansion of commercial surveillance has come to the attention of the Commission, and we are hopeful that it will produce a final rule that restores civil rights, reduces harm to consumers, promotes competition, and protects our democracy.

[2] https://www.accessnow.org/.

[3] [3] *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance*, Access Now (Jun. 7, 2021), https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf.

[4] Letter to Amazon Web Services concerning its hosting of the HART Biometric database, Access Now (May 24, 2022), https://www.accessnow.org/cms/assets/uploads/2022/05/Letter-to-AWS-re-hosting-of-HART-biometric-database_24-May-2022_Final.pdf.

[5] *Id*.

[6] https://reclaimyourface.eu/.

[7] https://act.accessnow.org/page/79916/action/1.

[8] https://www.accessnow.org/whyid/.

The RFC seeks answers to a variety of questions. This submission provides information in response to several questions, specifically questions 4, 27, 32, 37, 38, 43, and 47, and may apply to others.

This comment addresses how data collection practices cause significant harm to people; the role of data security; and the benefits of data minimization. It will also explore the exhibited and potential harms of particular biometric technologies, namely what emotion recognition technology is; the unreliability and discriminatory nature of emotion recognition technology; how emotion recognition undermines the rights to freedom of thought and privacy; how automated recognition of gender and sexual orientation is a threat to LGBT+ people; how mandatory digital identity programs using biometric recognition lead to exclusionary outcomes; and how biometric recognition is predicated on mass surveillance.

## III. Collecting Extensive Amounts of Data, Particularly Biometric Data, Causes Significant Harm (Relevant to question 4)

Expansive data collection practices have caused significant harm and risk of harm for millions of people.[9]These harms range from the more obvious identity theft and physical harms to less obvious examples, such as relationship harms (due to loss of confidentiality), emotional or reputational harms (due to private information becoming public), or chilling effects on speech or activity (due to a loss of trust in government or other organizations).[10] In this comment, we discuss some of the harms of the surveillance economy, but there are many more.

Particularly troubling are discrimination-related harms. Data collection and processing can “reduce opportunities for Black, Hispanic, Indigenous, and other communities of color, or actively target them for discriminatory campaigns and deception.”[11] During the 2016 election, the Russian Internet Research Agency used Facebook, and Twitter’s audience filters feature to target Black people to discourage them from voting.[12] Another study revealed that women, Black people, and Indigenous

[9] [9] Eric Null, Isedua Oribhabor, and Willmary Escoto, *Data Minimization: Key to Protecting Privacy and Reducing Harm*, Access Now (May 2021), https://www.accessnow.org/cms/assets/uploads/2021/05/Data-Minimization-Report.pdf.

[10] *Id*.

[11] Cameron F. Kerry, *Federal privacy legislation should protect civil rights*, Brookings Institute (Jul. 16, 2020), https://www.brookings.edu/blog/techtank/2020/07/16/federal-privacy-legislation-should-protect-civil-rights.

[12] Scott Shane and Sheera Frenkel, *Russian 2016 influence operation targeted African-Americans on social media,* The New York Times Magazine (Dec. 17, 2018), https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html; Jack Stubbs, *Facebook says Russian influence campaign targeted left-wing voters in U.S., UK*, Reuters (Sept. 15, 2020), https://www.reuters.com/article/usa-election-facebook-russia/facebook-says-russian-influence-campaign-targeted-left-wing-voters-in-u-s-uk-idUSKBN25S5UC; see also *Report of the Select Committee on Intelligence in the U.S. Senate on Russian Active Measures Campaigns and Interference in the 2016 Election, Volume 2: Russia’s Use of Social Media with Additional Views*, at 35, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf (a statement from Renee DiResta, Director of Research at New Knowledge, a cybersecurity company, indicated “Voter suppression narratives were … specifically targeting the Black audiences.”).

people are more likely to be victims of cybercrimes, particularly identity theft.[13] The Commission also found that "African American and Latino consumers were more likely to be fraud victims than non-Hispanic whites."[14]

Processing biometric data can lead to error and present extreme risks to privacy and civil rights. Biometric surveillance is becoming an all-encompassing tool for the companies to track where we are, what we are doing, and who we are with, regardless of whether an individual is suspected of a crime. For example, a mobile analytics company called Mobilewalla collected location data, device IDs, and browsing histories from over 16,000 devices in Black Lives Matter protests in major cities across the U.S. With that data, Mobilewalla used "artificial intelligence" to predict people's demographics like race, age, gender, and zip code. The protestors likely had no idea the company was collecting and processing data in such an intrusive way.[15]

Authorities in New York, Miami, South Carolina, Philadelphia, and Washington, DC, have also used facial recognition software to identify and arrest protestors.[16] In 2021, the Detroit Police Department overwhelmingly used FRT to find Black suspects. Out of 69 searches, the department: "used facial recognition software to identify 68 Black suspects and only one white suspect. That means police used facial recognition software to find Black suspects 98 percent of the time. The city is more than 80 percent Black."[17]

[13] Tonya Riley, *Cybercrime is hitting communities of color at higher rates, study finds*, Cyberscoop (Sept. 27, 2021), https://www.cyberscoop.com/cybercrime-demographics-bipoc-malwarebytes/.

[14] *Combating Fraud In African American & Latino Communities: The FTC's Comprehensive Strategic Plan: A Federal Trade Commission Report To Congress*, The Federal Trade Comission (Jun. 15, 2016), https://www.ftc.gov/system/files/documents/reports/combating-fraud-african-american-latino-communities-ftcs-comprehensive-strategic-plan-federal-trade/160615fraudreport.pdf.

[15] C. Fisher, *Demographic report on protests shows how much info our phones give away*, Engadget (Jun. 25, 2020), https://www.engadget.com/mobilewalla-data-broker-demographics-protests-214841548.html; Caroline Haskins, *Almost 17,000 Protesters Had No Idea A Tech Company Was Tracing Their Location*, Buzzfeed News (Jun. 25, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/protests-tech-company-spying.

[16] Justin Jouvenal, *Coalition of groups calls for end to facial recognition program used to identify protester at Lafayette Square*, The Washington Post (Apr. 28, 2021), https://www.washingtonpost.com/local/public-safety/facial-recognition-washington/2021/04/27/a6fb257c-a6c3-11eb-8d25-7b30e74923ea_story.html; Justin Jouvenal and Spencer S. Hsu, *Facial recognition used to identify Lafayette Square protester accused of assault*, The 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; Kate Cox*, Cops in Miami, NYC arrest protesters from facial recognition matches*, Ars Technica (Aug. 19, 2020), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches/.

[17] Bryce Huffman, *What we know so far about Detroit's controversial use of facial recognition*, Bridge Detroit (Jul. 21, 2021), https://www.bridgedetroit.com/what-we-know-so-far-about-detroits-controversial-use-of-facial-recognition/.

Similarly, in Los Angeles, the Police Department used Amazon Ring video cameras to monitor Black Lives Matter protests.[18] Posts on the Ring Neighbors app highlight the risks of anti-Black citizen vigilantism in expanding law enforcement's capacity to surveil Black and Brown people. In 2019, a *VICE Motherboard* investigation exposed the prevalence of discriminatory and racist comments on Neighbors app.[19] Out of more than 100 user-submitted posts over two months in the New York City area, those the app individuals most commonly reported as "suspicious" were people of color. In one instance, commenters encouraged an individual who posted a video to call the NYPD and suggested (without evidence) that a group of young "suspicious" Black boys planned to smoke crack.

Ring claims its Ring doorbell cameras do not have facial recognition, but seventeen patents granted to the company for its products "suggests the company is working towards using the doorbell cameras for biometric surveillance purposes."[20] The documents describe various biometric identification forms, including facial, palm, finger, retina, iris, typing, gait, and voice recognition. Ring was also awarded patents for using smell and skin texture to identify a "suspicious" person.[21] Days after Ring was awarded the patents, the New York University School of Law's Policing Project released the 'Ring Neighbors & Neighbors public safety service' report.[22] Following the publication of the Policing Project audit, Ring implemented new features and policy changes, including making all police requests for footage public and implementing anti-bias measures on the Neighbors apps.[23]

Companies are essential in shaping how private surveillance impacts public safety and civil liberties. While Ring's willingness to open itself up to an external audit is an example others should follow, all entities and companies need to be more forthcoming about what biometric data it collects, especially regarding face data. Commercial-police partnerships like these deserve greater scrutiny because they provide police with a much more expansive surveillance system than they could build and create incentives to place products in already overpoliced minority neighborhoods.

[18] Willmary Escoto, *Why We Don't like Amazon Ring*, Access Now (Dec. 15, 2021), https://www.accessnow.org/amazon-ring-privacy-review/; Matthew Guariglia and Dave Maass, *LAPD Requested Ring Footage of Black Lives Matter Protests*, Electronic Frontier Foundation (Feb. 16, 2021), https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests.

[19] Caroline Haskins, *Amazon's Home Security Company Is Turning Everyone Into Cops*, VICE (Feb. 7, 2019), https://www.vice.com/en/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops.

[20] Alessandro Mascellino, *Amazon Ring patents hint at biometric surveillance capabilitie*s, Biometric Update (Dec. 20, 2021), https://www.biometricupdate.com/202112/amazon-ring-patents-hint-at-biometric-surveillance-capabilities.

[21] Florence Ion, *In the Future, Amazon's Ring Doorbell Might Use Biometric Data to Surveil Neighborhoods*, Gizmodo (Dec. 16, 2021), https://gizmodo.com/in-the-future-amazons-ring-doorbell-might-use-biometri-1848230784.

[22] David Priest, *Ring's NYU Policing Project audit leads to Neighbors app changes*, CNET (Dec. 16, 2021),https://www.cnet.com/home/security/rings-nyu-policing-project-audit-leads-to-neighbors-app-changes/.

[23] *Id*.

A new report from the Electronic Privacy Information Center (EPIC) investigated Washington, DC's use of algorithms and found they were used across twenty agencies.[24] More than a third of these algorithms were deployed in policing or criminal justice. Notably, EPIC's project revealed evidence "that automated traffic-enforcement cameras are disproportionately placed in neighborhoods with more Black residents."[25] This is concerning for a myriad of reasons. We know that calling the police excessively results in fatal outcomes for Black and Brown people. The murder of Trayvon Martin and the prevalence of discriminatory and racist posts on the Amazon Ring Neighbors app illustrate the darker side of neighborhood watch programs and the citizen vigilantism we should avoid empowering.

The collection and use of biometric data poses significant risk to individuals and communities. In the past few years, a company that built a database of facial images illegally (and unethically) scraped from social media platforms and websites has come under intense scrutiny for its collection, use, and dissemination of biometric data and misrepresentations about its services. Clearview AI ("Clearview") is facing litigation, investigations, and severe backlash and class-action lawsuits for privacy violations all over the world and in several U.S. states including Illinois, California, Vermont, and New York.[26] Most recently, the CNIL, France's privacy watchdog, fined Clearview 20 million euros after the company failed to respond to an order last year to stop its unlawful processing of French citizens' information and delete their data.[27] Despite geographical differences, these cases raise similar alarms—Clearview does not care about consumer consent and poses serious risks to individual privacy.

Clearview uses "screen scraping" to capture the biometric information of images available online, all without the knowledge or consent of those pictured.[28] In addition to collecting and storing billions of photos, Clearview developed a facial recognition algorithm.[29] Clearview's scraping of websites does not distinguish between adults or children. Many of these websites, including Google, Twitter, YouTube, LinkedIn, and Facebook, contain terms of service with prohibitions on screen scraping and implement technology to attempt to prevent screen scraping.[30] Several social media companies like

[24] Thomas McBrien, Ben Winters, Enid Zhou, et.al, *Screened & Scored in DC*, EPIC (Nov. 2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf.

[25] Khari Johnson, *Algorithms Quietly Run the City of DC—and Maybe Your Hometown*, WIRED (Nov. 8, 2022), https://www.wired.com/story/algorithms-quietly-run-the-city-of-dc-and-maybe-your-hometown/.

[26] Nat Rubio-Licht, *ACLU settles landmark privacy lawsuit with Clearview AI*, Protocol (May 9, 2022), https://www.protocol.com/bulletins/aclu-clearview-ai-lawsuit; Rachel Metz, *Clearview AI sued in California by immigrant rights groups, activists*, CNN Business(Mar. 10, 2021), https://edition.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html; *Clearview Sued By Vermont Attorney General For Violating The State's Privacy Laws*, TechDirt (Mar. 11, 2020), https://www.techdirt.com/2020/03/11/clearview-sued-vermont-attorney-general-violating-states-privacy-laws/.

[27] Natasha Lomas, *France fines Clearview AI maximum possible for GDPR breaches*, TechCrunch (Oct. 20, 2022), https://techcrunch.com/2022/10/20/clearview-ai-fined-in-france/.

[28] *State v. Clearview AI Inc., No. 226-3-20, 2020 VT 4,* https://ago.vermont.gov/wp-content/uploads/2020/03/Complaint-State-v-Clearview.pdf.

[29] *Id*. at Para 24.

[30] *Id*. at Para. 33.

YouTube and Venmo already sent Clearview cease-and-desist letters for violating their terms of service.[31]

The American Civil Liberties Union (ACLU) initiated a case against Clearview under the Illinois Biometric Information Privacy Act (BIPA), which regulates the collection, use, and dissemination of biometric information.[32] The ACLU settled the lawsuit in Illinois, barring Clearview from selling its biometric data to most businesses and private firms across the United States. However, the company is still able to sell its algorithm (rather than access to its database) to private companies in the U.S. The settlement order also includes an exception for government contractors—suggesting Clearview can continue to work with federal government agencies in the U.S., like Homeland Security and the FBI—while applying a five-year ban on providing its software to any government contractors or state or local government entities in Illinois itself.

In Vermont, the Attorney General sued Clearview for violating the Vermont Consumer Protection Act which prohibits unfair and deceptive practices in commerce.[33] The Vermont trial court rejected Clearview's motion to dismiss and allowed the State Attorney General's lawsuit against Clearview to proceed. In March 2020, The Vermont Attorney General sent Clearview a cease-and-desist letter advising the company to: (1) cease collecting any photographs that include Vermont residents; and (2) delete or destroy all photographs and facial recognition identifiers of Vermont residents.[34]

The collection and use of biometric data, particularly face data, poses significant risks to individuals.[35] Because of this, the Commission should prioritize investigations and meaningful enforcement action of facial recognition vendors when privacy, data protection, and other rules have been violated through their products' development and use. Recently, the European Data Protection Board emphasized that

> *"[T]he processing of biometric data under all circumstances constitutes a serious interference in itself. This does not depend on the outcome, e.g. a positive matching. The processing constitutes an interference even if the biometric template is immediately deleted after the matching against a police database results in a no-hit."*[36]

[31] Gisela Perez and Hilary Cook, Google, *YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement*, CBS News (Feb. 5, 2020, 6:25 AM), https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/.

[32] 740 Ill. Comp. Stat. 14/5 (2018).

[33] *State v. Clearview AI Inc.*

[34] https://ago.vermont.gov/wp-content/uploads/2020/03/2020-03-05-Clearview-Letter-ID-227006.pdf.

[35] Access Now and over 175 civil society organizations, activists, and researchers from across the globe are calling for a ban on uses of facial recognition and remote biometric recognition that enable mass and discriminatory targeted surveillance, https://www.accessnow.org/civil-society-ban-biometric-surveillance/.

[36] *Access Now submission to the consultation on the European Data Protection Board's guidelines 05/2022 on the use of facial recognition technology in the area of law enforcemen*t, Access Now (Jun. 27, 2022), https://www.accessnow.org/cms/assets/uploads/2022/07/Access-Now-submission-to-the-consultation-on-the-European-Data-Protection-Boards-FRT-for-LEAs-guidelines-05_2022.pdf.

The EDPB also emphasized the chilling effect these technologies can cause: *"it is also not inconceivable that the collection, analysis and further processing of the biometric (facial) data in question might have an effect on the way that people feel free to act even if the act would be fully within the remits of a free and open society"*[37]

Moreover, because these technologies can process people's biometric data without their knowledge, they pose a particular threat and are even more prone to causing a chilling effect:

> *"[I]t has to be considered as a matter of severity, that if the data is systematically processed without the knowledge of the data subjects, it is likely to generate a general conception of constant surveillance. This may lead to chilling effects in regard of some or all of the fundamental rights concerned."*[38]

Given the proliferation of companies that have amassed extensive databases of people's biometric data by indiscriminately scraping the web, we welcome the Commission's dedication to protecting against unfair or deceptive practices related to biometrics.[39] We strongly encourage the Commission to adopt the EDPB's approach regarding the meaning of 'manifestly made public':[40]

- Paragraph 74 of the EDPB guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement importantly highlights that even if a photograph has been manifestly made public, this does not imply that the biometric data which can be extracted from that photograph has been manifestly made public: "the fact that a photograph has been manifestly made public by the data subject does not entail that the related biometric data, which can be retrieved from the photograph by specific technical means, is considered as having been manifestly made public."[41]
- Paragraph 76 also makes the important point that simply neglecting to activate certain privacy features on the part of the data subject is also not sufficient grounds to consider that their data has been manifestly made public: "the fact that the data subject did not trigger or set specific privacy features is not sufficient to consider that this data subject has manifestly made public its personal data and that this data (e.g. photographs) can be processed into biometric templates and used for identification purposes without the data subject's consent."[42]

[37] *Id*.

[38] *Id*.

[39] Evan Selinger, *A.I. Can't Detect Our Emotions*, One Zero (Apr. 6, 2021), https://onezero.medium.com/a-i-cant-detect-our-emotions-3c1f6fce2539; *Emotion Detection and Recognition Market 2022: Global Trends, Size, Share, Segments And Growth Forecast To 2029*, Market Watch (Jun. 3, 2022), https://www.marketwatch.com/press-release/emotion-detection-and-recognition-market-2022-global-trends-size-share-segments-and-growth-forecast-to-2029-2022-06-03.

[40] *Access Now submission to the consultation on the European Data Protection Board's guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.*

[41] *Id*.

[42] *Id*.

The FTC should take a more critical stance on penalties for companies that mislead consumers on the collection of biometric data by amplifying its use of algorithmic destruction. Access Now encourages the Commission to adopt this standard for penalizing tech companies that violate privacy and use deceptive data practices. The FTC first used the approach in 2019 when it ordered Cambridge Analytica to destroy the data it had gathered about Facebook users through deceptive means along with "information or work product, including any algorithms or equations" built using that data.

Algorithmic destruction or disgorgement came around again when the commission settled a case with photo-sharing app company Everalbum.[43] Then, in a settlement order, the Commission demanded that WW International — formerly known as Weight Watchers — destroy the algorithms or AI models it built using personal information collected through its Kurbo healthy eating app from kids as young as 8 without parental permission.[44] The agency also fined the company $1.5 million and ordered it to delete the illegally harvested data. The FTC should continue to slowly introduce this new type of penalty.

## IV. The Role of Data Security (Relevant to questions 27 and 32)

Once collected, lax data security practices have led to the unauthorized access to and use of personal information, compromising people worldwide. Data breaches are increasing in frequency and the U.S. suffers from the most data breaches. In 2021, 212.4 million individuals were affected by data breaches (compared to 174.4 million in 2020).[45] Data breaches are harmful to both individuals and companies. Not only does a data breach harm a company's reputation, but the average cost of a data breach can reach millions of dollars.[46] Data breaches are also often more problematic for Black and Brown people living on fixed or low incomes.[47] Therefore, mitigating widespread damage from data breaches to these communities is imperative for companies to restore consumer confidence.

Robust encryption is the next step toward protecting networks and data from unauthorized surveillance. Encryption is essential not only for protecting privacy, free expression, and other human

[43] *California Company Settles FTC Allegations It Deceived Consumers about use of Facial Recognition in Photo Storage App*, the Federal Trade Commission (Jan. 11, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo.

[44] *FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data*, FTC (Mar. 4, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive.

[45] *Data breach statistics by country in 2021*, Surfshark (Apr. 13, 2022), https://surfshark.com/blog/data-breach-statistics-by-country-in-2021

[46] *Cost of a Data Breach 2022 Report,* IBM (2022), https://www.ibm.com/security/data-breach.

[47] Kori Hale, *How T-Mobile's $350 Million Data Breach Settlement Still Leaves The Black Community At Risk*, Forbes (Aug. 3, 2022) https://www.forbes.com/sites/korihale/2022/08/03/how-t-mobiles-350-million-data-breach-settlement-still-leaves-the-black-community-at-risk/?sh=1624167e57a6; see also Hale, *T-Mobile's Hack Of 50 Million individuals Leaves Black Community At Risk*.

rights but also for bulwarking the economy, preserving democracy, and ensuring national security.[48] Intentionally undermining encryption would impede competition. It would inflict steep costs on companies that depend on it, and adversely impact the economy.[49]

The compliance burden imposed by laws to weaken encryption has compelled tech companies to retreat from the market in some countries.[50] This corporate withdrawal hurts competition and innovation and impacts employment.[51] If countries undermine encryption, their markets will lose companies that offer or depend on security products and services. Undermining encryption will inevitably disincentivize companies from innovating and developing such products.[52]

In 2014, Access Now launched the Encrypt All the Things campaign to encourage the widespread use of data security practices. The campaign's centerpiece is the Data Security Action Plan which includes seven security-enhancing steps that companies can take to provide a minimum amount of protection to personal data.[53] These steps ensure a minimum layer of data protection on private networks and communication channels:

1. **Implement strict encryption measures on all network traffic.** Transport layer security, or TLS, is a means to encrypt web traffic and authenticate websites to prevent so-called "man in the middle" attacks. When a server communicates with a browser using encryption, it becomes exceedingly difficult for an outside party to access the information passing over the internet. Strict transport security layer protocols cannot be downgraded to remove the encrypted layer. A best practice is maintaining strict transport layer security with perfect forward secrecy on all traffic, including internal traffic and traffic the server introduces to the individual.
2. **Executive verifiable practices to effectively store consumer data.** Data collected and stored by any entity, including information from or about individuals, should be protected. The current primary method of protection is through an encryption regime for all stored data, although other methods may be possible to reach the same result. Any method employed should be measurable to continually assess the security of the information. Existing data protection compliance regimes may provide guidance on security measures for data.
3. **Maintain the security of credentials and provide robust authentication safeguards.** Data breaches in online services have broadly impacted the privacy and security of people. Because many individuals still use easy-to-guess passwords or share passwords across multiple online accounts, these data breaches can be especially devastating to individuals. User credentials should never be stored in plain text but securely, for example, through hashing and salting using slow algorithms. This will ensure that should there be a data breach, passwords cannot

[48] Namrata Maheshwari and Raman Jit-Singh Chima,Why encryption is important: 10 facts to counter the myths, Access Now( Aug. 31, 201), https://www.accessnow.org/why-encryption-is-important/.
[49] *Id*.
[50] *Id*.
[51] *Id*.
[52] *Id*.
[53] *Encrypt All the Things*, Access Now (Mar. 4, 2014), https://www.accessnow.org/encrypt-all-the-things/.

be easily recovered. Two-factor authentication can help preserve the integrity of accounts but must be voluntarily implemented so that individuals who wish to maintain their anonymity may choose to do so.

4. **Promptly address known, exploitable vulnerabilities.** All vendors should have a patching regime to update servers with security patches. Patching regimes for client-side applications should be implemented properly to not introduce new vulnerabilities to the individual. Individuals should always have the option to make updating a manual process, subject to explicit consent. Updates that result in the greater collection of information should never be pushed through without clear and express notification and consent. Companies should be transparent about any vulnerabilities to which individuals have been or are currently exposed.
5. **Use algorithms that follow security best practices***.* Bad actors can exploit weak or insecure algorithms and implementations of algorithms to access otherwise protected information. To ensure that companies follow security best practices in protecting communications and data, they should disable the use of insecure algorithms and publicize which algorithms they use to ensure thorough vetting by the security community.
6. **Require companies to enable or support the use of end-to-end encryption.** Services that support the use of end-to-end encryption give individuals greater control to protect the security of communications. Using open protocols, not only can the security of the protocol be verified, but end-to-end secure communications can be built on top of those protocols.
7. **Provide education tools on the importance of digital security hygiene.** Protecting individual data and communications is only enough if individuals understand the risks they face, the rights they enjoy, and the different security options available to them. Education tools should empower individuals toward these goals.

Access Now believes in the importance of protecting networks, data, and consumers from unauthorized access and surveillance, and educating the public on the same. Entities should implement the seven steps of the Data Security Action Plan to increase the security and protection of information across the internet.

## V. Data Minimization Reduces Harm, Limits Surveillance, and Increases Data Security (Relevant to questions 43 and 47)

While data minimization defies any single definition, the simplest and most useful definition is that any organization (whether private company, public entity, or government body) collecting data should collect only the data necessary to provide their product or service, and nothing more. Minimizing data means collecting data only for an immediate and necessary purpose, not hoarding the data on the "off-chance that it might be useful in the future."[54] More specifically, organizations should limit (1) the scope of the data they collect, (2) the amount of data they collect within that

[54] International Commissioners Office, *Principle (c): Data minimisation,* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation.

narrow scope, and (3) the retention of that data.[55] One prominent example of the data minimization principle in action is “a data controller should not continuously process the precise and detailed location of the vehicle for a purpose involving technical maintenance or model optimization.”[56]

Organizations need to take data minimization seriously. They have collected and retained data with impunity, and many have failed to follow safeguards or to take a disciplined approach that protects individual privacy. One study of companies in Europe showed that 72% gathered data they ended up not using.[57] Another global report showed that 55% of all data collected is “dark data” that is not used for any purpose after being collected.[58] Data has become a commodity to many organizations, and few will change their business model in recognition of privacy being a human right.[59] The reasoning is clear: organizations want as much data as possible to monetize (through, for instance, behavioral advertising), track people, or make some other use of the data in the future, potentially to train a machine learning model or sell the information to a data broker or the government.

The primary responsibility for reducing the amount of and protecting the data collected by companies should be placed on the companies themselves. Companies should understand what data they need to provide their goods and services and only collect data within that specified need. A data minimization requirement would limit data collection and use to the purposes necessary for running the business and providing the services. For example, the Online Privacy Act of 2019 states “A covered entity may not collect more personal information than is reasonably needed to provide a product or service that an individual has requested.”[60]

A company may argue that collecting data for behavioral advertising is how it earns revenue; therefore, it must be collected. To address that argument, data collected primarily for advertising purposes should be deleted after a specific time —such a requirement would hopefully allow for data to be used for behavioral targeting for a brief period yet prevent companies from holding onto private

[55] First, “the *possibility* to collect personal data about others should be minimized,” then “within the remaining possibilities, *collecting* personal data should be minimized,” and finally, “*how long* collected personal data is stored should be minimized.” *Terminology for Talking about Data Minimization*, IETF (2010), https://tools.ietf.org/id/draft-hansen-privacy-terminology-00.html (emphasis added). Data retention is a closely related principle that ensures once data has served its purpose, the organization deletes the data.

[56] Commission Nationale Informatique & Libertes (NCIL), *Compliance Package - Connected Vehicles and Personal Data* (Oct. 2017), https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf at 10.

[57] *Big Data’s Failure: The struggles businesses face in accessing the information they need,* Pure Storage (July 2015), https://info.purestorage.com/rs/225-USM-292/images/Big%20Data%27s%20Big%20Failure_UK%281%29.pdf?aliId=64921319.

[58] *Companies Collect a Lot of Data, But How Much Do They Actually Use?*, Priceonomics, https://priceonomics.com/companies-collect-a-lot-of-data-but-how-much-do.

[59] Eric Null, *Ask Apple: Facebook Doesn’t Give a Damn about Privacy Protections*, Access Now (Mar. 29, 2021), https://www.accessnow.org/facebook-apple-privacy-war (explaining that Facebook and CEO Mark Zuckerberg were furious that Apple implemented a pro-privacy iOS update because it will affect Facebook and small businesses).

[60] https://www.congress.gov/bill/116th-congress/house-bill/4978/text

information indefinitely. Data collected primarily for advertising purposes also lose relevancy over time. For example, a profile may show that a person searched for or purchased maternity clothing. However, the person may receive targeted ads based on that history long after the need for maternity clothing passes.

Another risk of extensive data collection is the use of the information for government surveillance, which can lead to abuse of government authority and chilling effects on free expression. Data minimization can reduce those harms as well. When a government seeks information from a company like Signal, which offers end-to-end encryption of all communications (preventing any third party from viewing the contents of those communications) and keeps the data they collect about individuals to the bare minimum, the company has no information to give those authorities. When the U.S. government made such a request, including asking for the names and addresses of individuals, Signal responded that it "could not provide any of that. It is impossible to turn over data we never had access to in the first place."[61] If more companies adopted this kind of robust data minimization, fewer people would be subject to privacy violations, government surveillance, and abuse.

Data minimization is also an essential component of data security. Minimizing data collection practices means there will be less information at risk. As the unnecessary collection and retention of data increases, the growing treasure trove of data becomes a target for third parties, whether it is law enforcement or malicious hackers. Earlier this year Amazon responded to an inquiry from US Senator Ed Markey (D-Mass.), confirming that there have been 11 cases in 2022 where Ring handed over doorbell data to the police without  consumer consent.[62] Last year, Amazon's transparency report, which covers Amazon's shopping site as well as its Echo, Ring, and Fire products, showed an 800% increase in law enforcement requests for data in 2020 alone.[63] The spike is likely related to how much data Amazon holds about its individuals.

Organizations have the responsibility to secure and protect the data they process. The harm caused by data breaches, hacks, or unauthorized access to data within an organization is too great to justify collecting more data than is necessary to provide a product or service. Minimizing the amount of data companies collect is one of the best, most human rights-respecting ways to prevent privacy violations and harm. Requiring strong data minimization practices will have downstream effects, benefitting both individuals and companies. Storing data costs money. Companies can reduce their costs by only

[61] *Grand jury subpoena for Signal user data, Central District of California,* Signal (Apr. 27, 2021), https://signal.org/bigbrother/central-california-grand-jury.

[62] Ashley Belanger, *Amazon finally admits giving cops Ring doorbell data without user consent*, Ars Technica (Jul. 14, 2022), https://arstechnica.com/tech-policy/2022/07/amazon-finally-admits-giving-cops-ring-doorbell-data-without-user-consent/; Matthew Guariglia, *Senator Declares Amazon Ring's Audio Surveillance Capabilities "Threaten the Public*, The Electronic Frontier Foundation (EFF) (Jul. 14, 2022), https://www.eff.org/deeplinks/2022/06/senator-declares-concern-about-amazon-rings-audio-surveillance-capabilities; Jason Kelly and Matthew Guariglia, *Ring Reveals They Give Videos to Police Without User Consent or a Warran*t, EFF (Jul. 15, 2022), https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant.

[63] Zach Whittaker, *Amazon says government demands for user data spiked by 800% in 2021*, TechCrunch (Feb. 1, 2021), https://techcrunch.com/2021/02/01/amazon-government-demands-spiked.

collecting information necessary for their business. Moreover, the more personal information companies amass, the greater the risk of harm to an individual when a data breach occurs.

## VI. What is Emotion Recognition Technology? (Relevant to questions 37 and 38)

Facial recognition technology is frequently mentioned in discussions about biometrics, but many other biometric identification technologies are becoming more widely used. Despite questions from academics, activists, and scientists about whether emotion recognition technology ("ERT") works, this latest evolution in the broader world of artificial intelligence surveillance systems has continued to grow immensely and deserves greater scrutiny.

The term 'emotion recognition' covers a range of technologies that claim to infer someone's emotional state from data collected about that person.[64] Emotion recognition systems can be used in job interviews claiming to tell how enthusiastic or honest you are.[65] Airport security systems use emotion recognition to analyze your facial expressions for bad intent,[66] and if you are a defendant on trial, policing programs claim to detect deception.[67]

Emotion recognition is being deployed worldwide to make inferences about people's emotions, moods, and personalities, often without their consent or knowledge. From hiring,[68] education,[69] healthcare,[70] to policing.[71] The encroachment of ERT on people's rights in the United States has

[64] Jay Stanley, *Experts Say 'Emotion Recognition' Lacks Scientific Foundatio*n, ACLU (July 18, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/experts-say-emotion-recognition-lacks-scientific.

[65] Angela Chen and Karen Hao, *Emotion AI researchers say overblown claims give their work a bad nam*e, MIT Technology Review (Feb. 14, 2020), https://www.technologyreview.com/2020/02/14/844765/ai-emotion-recognition-affective-computing-hirevue-regulation-ethics/.

[66] Elaine Glusac, *What You Need to Know About Facial Recognition at Airports*, The New York Times (Feb. 26, 2022), https://www.nytimes.com/2022/02/26/travel/facial-recognition-airports-customs.html.

[67] Sebastien Krier, *Facing Affect Recognition*, (Sept. 18, 2020), https://asiasociety.org/sites/default/files/inline-files/Affect%20Final.pdf; https://emojify.info/.

[68] Douglas Perry*, Emotion-recognition technology doesn't work, but hiring professionals, others are using it anyway: report*, The Oregonian (Dec. 16, 2019), https://www.oregonlive.com/business/2019/12/emotion-recognition-technology-doesnt-work-but-hiring-professionals-others-are-using-it-anyway-report.html; Minda Zetlin, *AI Is Now Analyzing Candidates' Facial Expressions During Video Job Interviews*, Inc. Magazine, https://www.inc.com/minda-zetlin/ai-is-now-analyzing-candidates-facial-expressions-during-video-job-interviews.html.

[69] Michael Standaert*, Smile for the camera: the dark side of China's emotion-recognition tech*, The Guardian (Mar. 3, 2019), https://www.theguardian.com/global-development/2021/mar/03/china-positive-energy-emotion-surveillance-recognition-tech.

[70] Marwan Dhuheir, Abdullatif Albaseer, Emna Baccour, et. al., *Emotion Recognition for Healthcare Surveillance Systems Using Neural Networks: A Survey*, Cornell University (Jul. 13, 2021), https://arxiv.org/abs/2107.05989.

[71] Ismat Ara*, Lucknow Police to Use AI Cameras to Track Women's Distress, Activists Slam Privacy Invasion*, The Wire (Jan. 22, 2021), https://thewire.in/women/uttar-pradesh-lucknow-police-artificial-intelligence-camera-women; Alex Engler, *Why President Biden should ban affective computing in federal law enforcemen*t, Brookings (Aug. 4,

seemingly been harmless, with companies like Spotify and Zoom using it to manipulate our feelings for-profit and make biased inferences about us.[72] The comfort of having a song recommendation or “knowing" how an employee feels during a meeting may seem innocent. However, this technology raises serious human rights concerns that cannot be overlooked.

Many 'face-based' emotion recognition applications rely on the assumption that everyone expresses emotion in the same way. These emotion recognition systems rely on Paul Eckman's controversial 'basic emotions' theory. This theory posits 'universal categories' of human emotion and claims to describe how these can be read from facial expressions.[73] Furthermore, these systems often have the implicit or express intention of manipulating our thoughts by tailoring content to our emotional state.[74]

## VII. Emotion Recognition is Unreliable and Biased (Relevant to questions 37 and 38)

A prominent study by researchers in the science of emotion concluded that despite “[t]technology companies [...] investing tremendous resources to figure out how to objectively “read” emotions in people by detecting their presumed facial expressions [...] the science of emotion is ill-equipped to support any of these initiatives.”[75] Further, devastating criticism of the entire project of emotion recognition has been voiced from numerous quarters, with even Paul Eckman, whose theories underlie most of face-based emotion recognition systems, stating that “[m]ost of what I was seeing was what I would call pseudoscience” in emotion recognition technology.[76]

The relationship between facial expressions and a person's emotional state is much more complex than it might appear because people express their emotions differently across cultures, ethnicities, and circumstances. This is corroborated by researchers from the University of Glasgow, who found

2021), https://www.brookings.edu/blog/techtank/2021/08/04/why-president-biden-should-ban-affective-computing-in-federal-law-enforcement/.

[72] *Dear Spotify: don’t manipulate our emotions for profit*, Access Now (Apr. 15, 2021), https://www.accessnow.org/spotify-tech-emotion-manipulation/; Mack DeGeurin, *27 Rights Groups Demand Zoom Abandon 'Invasive,' and 'Inherently Biased' Emotion Recognition Software*, Gizmodo (May 11, 2022), https://gizmodo.com/zoom-emotion-recognition-software-fight-for-the-futur-1848911353.

[73] Oscar Schwartz, *Don’t look now: why you should be worried about machines reading your emotions*, The Guardian (Mar. 6, 2019), https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science.

[74] See, for example, this case taken by the Brazilian consumer organization, IDEC, where such a system was used in a metro line in São Paulo. Access Now intervened, submitting an expert opinion, and the judge ultimately ruled in favor of IDEC: https://www.accessnow.org/sao-paulo-court-bans-facial-recognition-cameras-in-metro/

[75] Lisa Feldman Barrett, et al, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, Psychological Science in the Public Interest, vol. 20, no. 1, pp. 1–68 (Jul. 2019), https://journals.sagepub.com/doi/10.1177/1529100619832930.

[76] Madhumita Murgia, *Emotion recognition: can AI detect human feelings from a face?* The Financial Times (May 12, 2021),https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452; Luke Stark and Jevan Hutson, *Physiognomic Artificial Intelligence*, Fordham Intellectual Property, Media & Entertainment Law Journal, (Sept. 20, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3927300.

that culture shapes the perception of emotions.[77] Facial expressions are filtered through culture to gain meaning, and our culture and societal attitudes fundamentally shape our emotions.[78] In addition, facial expressions do not always reflect our inner emotions because people often mask or suppress their emotions.[79]

Researchers from the University of Cambridge who designed a game that attempts to identify emotions from facial expressions concluded "that the software's readings are far from accurate, often interpreting even exaggerated expressions as 'neutral.'"[80] The game, emojify.info, challenges you to produce six emotions (happiness, sadness, fear, surprise, disgust, and anger), which the system will "read" by your computer via your webcam and attempt to identify.[81] This study demonstrates that "the basic premise underlying much emotion recognition tech: that facial movements are intrinsically linked to changes in feeling, is flawed."[82]

Emotion recognition technology is also racially biased. Research shows that some emotion recognition technology has trouble identifying the emotions of darker-skinned faces. In one study, emotion recognition systems assigned more negative emotions to Black men's faces when compared to white men's faces. These systems read Black men's faces as angrier than white men's, no matter their expression.[83]

The use of emotion recognition systems in hiring interviews,[84] schools,[85] and other settings have also caused great concern.[86] In China, emotion recognition has been used by teachers to monitor students'

[77] Chaona Chen et al., *Distinct Facial Expressions Represent Pain and Pleasure Across Cultures*, Proceedings of the National Academy of Sciences of the United States of America, vol. 115, no. 43, 2018, pp. E10013–E10021, https:// www.pnas.org/content/115/43/E10013.

[78] Michael Price, *Facial Expressions – Including Fear – May Not Be As Universal As We Thought*, Science ( Oct. 17, 2016),https://www.science.org/content/article/facial-expressions-including-fear-may-not-be-universal-we-thought ; Carlos Crivelli, James A. Russell, Sergio Jarillo, et al., *The Fear Gasping Face as a Thread Display in a Melanesian Society*, Proceedings of the National Academy of Sciences of the United States of America ( Oct. 17, 2016) ,https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5098662/.

[79] Miho Iwasaki and Yasuki Noguchi, *Hiding true emotions: Micro-expressions in eyes retrospectively concealed by mouth movements*, Scientific Reports (2016), https://www.nature.com/articles/srep22049.

[80] James Vincent, *Discover the stupidity of AI emotion recognition with this little browser game*, The Verge (Apr. 6, 2021), https://www.theverge.com/2021/4/6/22369698/ai-emotion-recognition-unscientific-emojify-web-browser-game; *Emojify*, https://emojify.info/

[81] Vincent, *Discover the stupidity of AI emotion recognition with this little browser game.*

[82] *Id*.

[83] Lauren Rhue, *Emotion-reading tech fails the racial bias test*, The Conversation (Jan 3, 2019), https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404.

[84] Sheridan Wallar and Schellmann*, We tested AI interview tools. Here's what we found*, MIT Technology Review (July 7, 2021), https://www.technologyreview.com/2021/07/07/1027916/we-tested-ai-interview-tools/.

[85] Milly Chan, *This AI reads children's emotions as they learn*, CNN Business (Feb. 17, 2021), https://www.cnn.com/2021/02/16/tech/emotion-recognition-ai-education-spc-intl-hnk/index.html ; https://restofworld.org/2021/chinas-emotion-recognition-tech/.

[86] Cheryl Teh, *'Every smile you fake' — an AI emotion-recognition system can assess how 'happy' China's workers are in the office*, Insider (Jun. 15, 2021),

emotions as they study at home and gauge how they respond to classwork.[87] As they study, the system collects specific biometric information (like the muscle points on their faces) through the camera on their computer or tablet.[88] The system then attempts to identify emotions such as happiness, sadness, anger, surprise, and fear.[89]

This technology presents real harm to marginalized communities.[90] Using emotion recognition systems in education could further exacerbate existing oppressive dynamics. For instance, it is common knowledge that Black students experience more suspensions and other disciplinary actions than white students, often for the same behavior.[91] Another study exploring the racialized perception of emotions and bias among prospective teachers concluded that the teachers are more likely to interpret Black boys' and girls' facial expressions as angry, even when they are not.[92] If racially biased emotion recognition technology is deployed in these problematic situations, existing inequalities and oppression could be magnified.

## VIII. Emotion Recognition Undermines the Right to Privacy, Freedom of Thought and Expression (Relevant to questions 37 and 38)

Technology that makes inferences about our emotional state represents an unacceptable intrusion into our private mental life and erodes our right to privacy and freedom of thought.[93] The right to freedom of thought includes the right to keep our thoughts and opinions private, the right not to have our thoughts and opinions manipulated, and the right not to be penalized for our thoughts and opinions.[94]

As the organization Article 19 pointed out, emotion recognition applications are a highly invasive form of surveillance that track, monitor, and profile individuals through overt collection of sensitive

https://www.insider.com/ai-emotion-recognition-system-tracks-how-happy-chinas-workers-are-2021-6.

[87] Chan, *This AI reads children's emotions as they learn.*

[88] *Id.*

[89] *Id.*

[90] Abeba Birhane, *The Impossibility of Automating Ambiguity,* Artificial Life (Jun. 11, 2021) https://direct.mit.edu/artl/article-abstract/27/1/44/101872/The-Impossibility-of-Automating-Ambiguity?redirectedFrom=fulltext.

[91] Travis Riddle and Stacey Sinclair, *Racial disparities in school-based disciplinary actions are associated with county-level rates of racial bias*, Princeton University (Apr. 2, 2019), https://www.pnas.org/content/116/17/8255.

[92] Amy G. Halberstadt et al., *Racialized Emotion Recognition Accuracy and Anger Bias of Children's Faces*, American Psychological Association (2020), https://www.apa.org/pubs/journals/releases/emo-emo0000756.pdf; Amy Halberstadt and Matt Shipman*, Future Teachers More Likely to View Black Children as Angry, Even When They Are Not*, NC State University (July 6, 2020), https://news.ncsu.edu/2020/07/race-anger-bias-kids/.

[93] *Access Now submission to the UN Special Rapporteur on Freedom of Religion or Belief Call for Inputs: Report to the UN General Assembly 76th Session on Respecting, Protecting and Fulfilling the Right to Freedom of Thought* (Jun. 30, 2021), https://www.accessnow.org/cms/assets/uploads/2021/11/UN-Special-Rapporteur-on-Freedom-of-Religion-or-Belief_-Consultation-on-freedom-of-thought-technology.pdf.

[94] Susie Alegre, *Protecting Freedom of Thought in the Digital Age*, Centre for International Governance Innovation (May 2021), https://www.cigionline.org/static/documents/PB_no.165.pdf.

personal data.[95] In her 2021 annual report on *The Right to Privacy in the Digital Age*, the UN High Commissioner for Human Rights notes that the "the use of emotion recognition systems by public authorities, for instance, for singling out individuals for police stops or arrests or to assess the veracity of statements during interrogations, risks undermining human rights, such as the rights to privacy, to liberty and to a fair trial" and that a "risk-proportionate approach to legislation and regulation will require the prohibition of certain A.I. technologies, applications or use cases, where they would create potential or actual impacts that are not justified under international human rights law, including those that fail the necessity and proportionality tests."[96]

Similarly, in their Joint Opinion on the European Union's Artificial Intelligence Act, the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) state that the "use of A.I. to infer emotions of a natural person is highly undesirable and should be prohibited."[97] While the EDPB-EDPS statement further notes that exceptions should be made for "certain well-specified use-cases, namely for health or research purposes," the fact that these systems are based on flawed scientific premises suggests that they should not be allowed in sensitive domains such as health.[98]

A particularly acute risk to human rights occurs if emotion recognition systems are used to detect potentially dangerous or aggressive protesters, leading to the arrest of these people before they have committed any illegal act.[99] In such a case, it would not matter whether the inference was unreliable; the consequences of arrest are real and would undermine a person's rights to freedom of expression and assembly.

## IX. Automated Recognition of Gender and Sexual Orientation Threated LGBT+ people (Relevant to questions 37 and 38)

Automatic Gender Recognition (AGR) aims to infer the gender of individuals from data collected about them. AGR uses information, like a legal name or the bone structure of your face, to infer your gender identity, often reducing it to a simplistic binary.[100]

AGR not only fails to reflect any objective or scientific understanding of gender, but it indirectly symbolizes a form of erasure for people who are trans or non-binary. Studies have shown that women

[95] *Emotional Entanglement: China's emotion recognition market and its implications for human rights*, Article 19 (Jan. 2021), https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.

[96]UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, A/HRC/48/31, UN Human Rights Council, 48th Session (Sept. 13, 2021), https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalReports.aspx.

[97] Natasha Lomas, *EU's data protection adviser latest to call for ban on tracking ads*, TechCrunch (Nov. 19, 2021), https://techcrunch.com/2021/11/19/edpb-call-to-ban-tracking-ads/.

[98] *Id.*

[99] Thomas Macaulay, *British police to trial facial recognition system that detects your mood,* TNW News (Aug. 17, 2020) https://thenextweb.com/news/british-police-to-trial-facial-recognition-system-that-detects-your-mood

[100] OS Keyes, *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition*, Proceedings of the ACM on Human-Computer Interaction (Nov. 2018), https://ironholds.org/resources/papers/agr_paper.pdf.

of color, particularly Black and transgender people, are at a higher risk of misgendering.[101] Furthermore, inferring gender on a binary scale erases the existence of non-binary people and has real-world consequences. Simply put—when communities are systematically misrepresented, their ability to advocate effectively for their human rights and freedoms are crippled.[102]

In 2021, hundreds of human rights groups, recording artists, and academics penned an open letter to Spotify, requesting that the company not use their patented technology to listen to individuals' conversations and recommend content based on their perceived emotions.[103] Spotify's speech-recognition patent[104] claims to be able to detect,[105] among other things, "emotional state, gender, age, or accent" to recommend music better. In other words, Spotify's technology uses emotion recognition and gender recognition to make inferences about what emotion a person is experiencing and what gender they are to recommend a song. According to the patent, the device would stay on all the time, constantly monitoring, processing voice data, and collecting sensitive information.[106] It could even detect the number of people in a room.

Automated recognition of gender and sexual orientation can cause numerous harms to LGBT+ people. LGBT+ people could be interrogated by authorities at the airport if the system determines you do not match the gender marker in your passport. On the same basis, a transgender person could be prohibited from access to gender-specific spaces like bathrooms and locker rooms. Authorities in repressive countries could analyze security camera footage or social media profiles to track down individuals they believe to be LGBT+ and arrest them.[107]

## X. Mandatory Digital Identity Programs using Biometric Recognition lead to Exclusionary Outcomes (Relevant to questions 37 and 38)

Governments and companies are leveraging biometric technologies to identify and authenticate ill-considered, badly designed, and poorly implemented digital identity programs.[108] Often, these digital identity programs are mandatory.[109] Most of these enrollment systems capture personal information

[101] http://gendershades.org.

[102] Daniel Leufer, *Computers are binary, people are not: how AI systems undermine LGBTQ identity*, Access Now (Apr. 6, 2021), https://www.accessnow.org/how-ai-systems-undermine-lgbtq-identity/.

[103] Todd Feathers, *Artists Are Telling Spotify To Never Use 'Emotion Recognition,'* VICE News (May 5, 2021), https://www.vice.com/en/article/7kvvka/artists-are-telling-spotify-to-never-use-emotion-recognition.

[104] *Identification of taste attributes from an audio signal*, Justia (Feb. 21, 2018), https://patents.justia.com/patent/10891948.

[105] Mark Savage, *Spotify wants to suggest songs based on your emotions*, BBC News (Jan. 28, 2021) https://www.bbc.com/news/entertainment-arts-55839655.

[106] *Identification of taste attributes from an audio signal.*

[107] https://campaigns.allout.org/ban-AGSR.

[108] Veronica Arroyo and Donna Wentworth, *We need to talk about digital ID: why the World Bank must recognize the harm in Afghanistan and beyond*, Access Now (Oct. 14, 2021), https://www.accessnow.org/digital-id-world-bank/.

[109] *National Digital Identity Programmes: What's Next?*, Access Now (May 2018), https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf.;

along with biometrics. Introducing such a program jeopardizes human rights, particularly for political and religious minorities, and exposes them to threats from third parties.[110] In many places, populations, including refugees, transgender people, and those affected by HIV, are forced to register in digital identity programs as a pre-condition to receiving aid.[111]

There are also privacy concerns related to these digital identity programs. For example, the Intercept[112] reported that an Afghanistan Automated Biometric Identification System[113] maintained by the Afghan Ministry of the Interior *with* support from the U.S. government was seized by the Taliban. The devices, known as HIIDE, for Handheld Interagency Identity Detection Equipment, collected sensitive biometric data (such as iris scans, fingerprints, and other biographical information) on Afghan criminals, terrorists, and those who assisted the U.S. (or worked with the military).

## XI. Biometric Recognition is Predicated on Mass Surveillance (Relevant to questions 37 and 38)

Biometric recognition systems have "the capacity to identify, follow, single out, and track people everywhere they go, undermining our human rights and civil liberties."[114] These systems infringe on the rights to privacy and data protection, the right to freedom of expression, the right to free assembly and association (leading to the criminalization of protest and causing a chilling effect), and the rights to equality and non-discrimination.[115]

Still, many governments are eagerly purchasing the dangerous technology and ramping up implementation—even as the movement to ban facial recognition and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance gains traction

*Mandatory National IDs and Biometric Databases*, Electronic Frontier Foundation, https://www.eff.org/issues/national-ids.

[110] *Busting The Dangerous Myths Of Big Id Programs: Cautionary Lessons from India*, Access Now (Oct. 2021), https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf; Carolyn Tackett and Naman M. Aggarwal, *Government responses to COVID-19 reinforce the need to ask — #WhyID?,* Access Now (Apr. 29, 2020) https://www.accessnow.org/government-responses-to-covid-19-reinforce-the-need-to-ask-whyid/; *Civil society organizations call for a full integration of human rights in the deployment of digital identification systems,* Access Now (Dec. 17, 2020), https://www.accessnow.org/civil-society-call-for-human-rights-in-digital-identification-systems/; *#WhyID: Digital health certificates are not immune from violating individuals' rights*, Access Now (July 22, 2020), https://www.accessnow.org/whyid-digital-health-certificates-are-not-immune-from-violating-individuals-rights.

[111] *Iris scanning of refugees is disproportionate and dangerous — What's happening behind IrisGuard's closed doors?* Access Now (Apr. 12, 2021), https://www.accessnow.org/irisguard-refugees-jordan/.

[112] Ken Klippenstein and Sara Sirota, *The Taliban Have Seized U.S. Military Biometrics Devices*, The Intercept (Aug. 17, 2021), https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/.

[113] *Mission Afghanistan: Biometrics*, FBI (Apr. 29, 2011), https://www.fbi.gov/news/stories/mission-afghanistan-biometrics.

[114] *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance*.

[115] *Id.*

worldwide.[116] Biometric recognition technologies have already enabled a litany of human rights abuses, including the right to privacy, and  free assembly and association in the United States and China, Russia, England, Kenya, Slovenia, Myanmar, Israel, India, and the United Arab Emirates.[117]

Wrongful arrests in the United States, Argentina, and Brazil have undermined people's right to privacy, due process, and freedom of movement. So far, three Black men have been wrongfully arrested based on flawed facial recognition in the United States.[118] Similarly, the surveillance of ethnic and religious minorities and other marginalized and oppressed people in China, Thailand, and Italy have violated people's right to privacy, equality, and non-discrimination.[119]

Access Now and 193 civil society organizations from 63 countries worldwide called for a ban on using these technologies in publicly accessible spaces.[120] A moratorium could temporarily stop the development and use of these technologies and buy time to gather evidence and organize the democratic discussion. However, it is already clear that these investigations and discussions will only further demonstrate that using these technologies in publicly accessible spaces is incompatible with our human rights and civil liberties. They must be banned outright and for good.

Facial recognition and remote biometric recognition technologies have severe technical flaws in their current forms, including, for example, facial recognition systems that reflect racial bias and are less accurate for people with darker skin tones. However, technical improvements to these systems will not eliminate the threat they pose to our human rights and civil liberties. While adding more diverse training data or taking other measures to improve accuracy may address some current issues with these systems, this will only perfect them as surveillance instruments and make them more effective at undermining our rights.

## XII. Recommendations to the FTC (Relevant to questions 37, 38, 43, and 47)

Protection from commercial surveillance is critical to human- and civil-rights. The mass collection of data and the use of that data to track and influence people's choices creates a myriad of harms. These practices disproportionately harm Black and Brown communities by restricting opportunity and access, raising prices, and increasing surveillance and law enforcement.[121] Because of this, **Access Now urges the FTC to define and include a list of binding data protection principles in the law.**

[116] *Id*; Arroyo and Pisanu, *Surveillance Tech in Latin America: Made Abroad, Deployed at Home*.

[117] *See Open letter calling for a global ban.*

[118] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, New York Times (Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[119] *Id.*; *Alibaba facial recognition tech specifically picks out Uighur minority*, Reuters (Dec. 17, 2020), https://www.reuters.com/article/us-alibaba-surveillance-idUKKBN28R0IR.

[120] *See Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance.*

[121] For harms from algorithms see Jane Chung, *Racism In, Racism Out: A Primer on Algorithmic Racism*, Public Citizen (2020). https://www.citizen.org/news/report-algorithms-are-worsening-racism-bias-discrimination/.

Together with clear definitions, **the following eight following principles are at the core of data protection frameworks**. Put together, these interconnected principles make clear the necessary measures that any data protection framework which seeks to effectively protect individuals' rights should include. The effective codification of these principles requires the development of a set of individuals' rights, legal basis for data processing, data security measures, oversight mechanisms, obligations for entities processing data, and of measures enabling the transfer of data to third countries.

1. **Fairness and lawfulness:** Personal data should be processed on a clear legal basis, for a lawful purpose, and in a fair and transparent manner so that individuals are informed about how their data will be collected, used, or stored, and by whom.
2. **Purpose limitation:** Companies should collect and process data only for a specified and lawful purpose. This purpose should be specific, explicit, and limited in time. Data should not be further processed in any manner incompatible with that purpose.
3. **Data minimization:** Personal data collected and used should be limited to what is adequate, relevant, and not excessive in relation to a specific and defined purpose.
4. **Accuracy**: Personal data should be accurate and, where necessary, kept up to date. Individuals should have the right to erase, rectify, and correct their personal information.
5. **Retention limitation:** Personal data processed for any purpose should not be kept for longer than is necessary.
6. **Consumer rights:** Personal data should be processed in accordance with the rights of individuals such as the right to access or right to erasure (See point 4).
7. **Integrity and confidentiality:** Personal data should be processed in a manner that ensures state-of- the-art security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.
8. **Adequacy:** Personal data should not be transferred to a third country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data. Data protection frameworks should provide for mechanisms enabling the free flow of data between countries while safeguarding a higher level of data protection.

These eight data protection principles derive from international standards, in particular the Convention 108 and the OECD guidelines.[122] They are considered "as minimum standards" for the protection of fundamental rights by countries that have ratified international data protection frameworks. These principles should be the basis of any data protection framework and are present in data protection laws around the world, from the EU Data Protection Directive from 1995, the GDPR, and most data protection laws that are in place in Latin America.

[122] *Guidelines governing the protection of privacy and transborder flows of personal data*, Organisation for Economic Cooperation and Development (Sept. 1980) https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf.

**We also urge the FTC to define the legal basis authorizing data to be processed.** Any data protection framework must clearly define the legal basis under which individuals' personal data can be processed. Any entity, public or private, seeking to process personal data should abide by at least one of the legal bases provided for in the law. These usually include the execution of a contract, compliance with a legal obligation, and consent.

Consent should be defined as an active, informed, and explicit request from the individual. It must be freely given, and the individual must have the capacity to withdraw consent at any time. This means, for instance, that pre-ticked boxes would not qualify as valid consent. In addition, companies should not deny an individual access to a service for refusing to share more data than strictly necessary. Otherwise, consent would not be freely given.

**The FTC should also include a list of binding individuals' rights in the law.** Protecting users' data protection and guaranteeing their control over their personal information requires establishing a series of binding rights to exercise:

1. **Right to access** enables consumers to obtain confirmation from services and companies as to whether personal data concerning them have been collected and are being processed. If that is the case, consumers should have access to the data, the purpose for the processing, by whom it was processed, and more.
2. **Right to object** enables consumers to say "no" to the processing of their personal information when they have not given their consent to the processing of their data nor signed a contract. This right to object applies to automated decision-making mechanisms, including profiling, as consumers have the right not to be subjected to the use of these techniques.
3. **Right to erasure** allows individuals to request the deletion of all personal data related to them when they leave a service or application.
4. **Right to rectification** allows consumers to request the modification of inaccurate information about them.
5. **Right to information** ensures that individuals receive clear and understandable information from entities processing their personal data, whether these entities have collected this information directly or received it through third parties. Companies should provide consumers with information that is in a concise, intelligible, and easily accessible form. Companies should also use clear and plain language. This information should include details about data being processed, the purpose of this processing, and the length of storage. Companies should also provide their contact details and an email address to allow individuals to contact them in case there are issues.
6. **Right to explanation** empowers individuals to obtain information about the logic involved in any automatic personal data processing and the consequences of such processing. This right is crucial to bring accountability and transparency in the use of algorithms to make decisions that impact individuals' lives.
7. **Right to portability** enables individuals to move certain personal data they have provided from one platform to another offering similar services. To facilitate this process, interoperability between services should be encouraged.

Most importantly, **the FTC should develop rules that impose limitations on companies' collection, use, and retention of consumer data.** Accordingly, any framework aiming to protect personal information must include a clear definition of personal and sensitive data. The level of protection should correspond with the sensitivity of each category of data. The FTC should define sensitive data to include genetic and biometric data, as well as communications content and metadata, as this information reveals particularly sensitive personal traits. This means that a data protection framework should also include specific measures for the protection of data exchanged during communications and related privacy provisions to guarantee the confidentiality of communications.

Data minimization, purpose limitation, data security and transparency are not interchangeable principles. Each data protection principle is as important as the other, yet they overlap and complement one another, allowing businesses to operate with confidence and reassure people that they and their information is safe. There is also no limitation to the principles of data minimization and purpose limitation. These principles ensure that services, including essential services, have the data they need to function properly: no more, but also no less. These principles are never about not using data at all but ensuring that the data collected and used is needed.

We also invite the Commission to develop rules that restrict "further processing" use of data for different purposes or by different actors. For instance, if a consumer provides data to her insurance company for the purposes of processing her insurance contract, the company should not be able to pass along her data to any other company. The company should also be restricted from using the data themselves to start sending the consumer ads (if the company wants to do that, they need to ask separately and obtain separate consent).

**Furthermore, Access Now calls on the Commission to develop robust rules that protect data security and integrity**. It is time for the Commission to expand public discourse beyond transparency to include a conversation about securing data on private networks properly. **All entities should support the implementation of the seven security measures in the Data Security Action Plan on all relevant data and networks under their control.** Widespread adoption would benefit people using the internet worldwide and raise the floor on minimally acceptable data security practices.

The GDPR codifies the principles of data protection by design and by default, such as contributing to data security and integrity.[123] With privacy and data protection by design and by default, companies take a positive approach to protecting individuals' rights, by embedding privacy-protecting principles into both technology and organizational policy. Privacy and data protection becomes part of the company culture and accountability framework, rather than being a “simple” compliance element.

[123] See Article 25. European Union, Regulation 2016/679/EU on the protection of natural per- sons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), http://eur-lex.europa.eu/le- gal-content/EN/TXT/?uri=CELEX%3A32016R0679.

This requires thinking about privacy and data protection from the beginning of the process of developing a product or service.[124]

This approach can help companies save on development costs for products or services. Because engineers and development teams will have considered privacy and data protection at the outset of the development phase, there would be fewer adjustments that would have to be made when a legal team reviews the final product. It also reduces the risk of a company being sued for privacy violations or suffering reputational damage due to data leaks, as it would be able to demonstrate its commitment to individuals' rights. In short, moving from understanding privacy and data protection as a compliance issue to embedding privacy and data security by design and by default can help companies increase trust in their services. While data protection frameworks should encourage measures fostering data security and data integrity, data breaches can still take place. Therefore, measures to address, remedy, and notify individuals of such problems should therefore be put in place.

Human rights harms are inevitable when we allow companies to sell flawed technology. Without a robust process to validate the claims made by corporations selling these systems, we risk a proliferation of pseudoscientific technologies, damaging consumer confidence and public trust. For all these reasons**, we encourage the FTC to also use its *full* authority to protect persons against biometric systems**. This includes prohibiting the use of these technologies in public spaces, publicly accessible spaces, and places of public accommodation, where such use could enable mass surveillance or discriminatory targeted surveillance, including but not limited to their use in parks, schools, libraries, workplaces, transport hubs, sports stadiums, and housing developments.

When biometric technology is used to infer gender, it limits the ability of a person to self-identity. It puts companies in a dangerous position of power in relation to people using the service.  Spotify, for example, is incentivized to manipulate a person's emotions in a way that encourages them to continue listening to content on its platform—which could look like playing on a person's depression to keep them depressed. Accordingly, **some biometric technologies such as automated gender recognition and A.I.-based "detection" of sexual orientation must be banned outright.** Companies cannot fix these systems by introducing more diverse training data, increasing accuracy, or applying technical methods to reduce bias; the fundamental aim of these systems is incompatible with human rights.

**Finally, Access Now calls on the FTC to prioritize investigations and meaningful enforcement action of facial recognition vendors when privacy, data protection, and other rules have been violated through their products' development and use**. The Commission should **take a more critical stance on penalties for companies that mislead consumers on the collection of biometric data** by **amplifying the use of algorithmic disgorgement** (or algorithmic destruction) as an enforcement tool.

[124] For more information on Privacy by Design see Ann Cavoukian, *Privacy by Design*, the 7 Founda- tional Principles https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

When companies use deceptive data practices to build algorithmic systems like A.I. and machine-learning models, the punishment should be clear: They must destroy ill-gotten data and the models built with it. Like the penalty applied in Everalbum, any entity that engages in such practices should be forced to delete all photographs, videos and biometric data obtained through its application, and to remove "any models or algorithms developed, in whole or in part" using such data.

Respectfully Submitted,

Willmary Escoto, Esq. (CIPP/E)
U.S. Data Protection Lead
Access Now