17 November 2022

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

Re: Commercial Surveillance ANPR, R111004

IEEE-USA is pleased to submit public comments on the advanced notice of proposed rulemaking on the prevalence of commercial surveillance and data security practices that harm consumers. The information provided below is an effort of IEEE-USA, which represents the approximately 150,000 IEEE members in the United States. Our members include engineers, scientists, and other technical professionals who are actively conducting research and development into artificial intelligence (AI), software engineering, cybersecurity, and advanced computing. IEEE Standards Association (IEEE SA) is developing technical standards and frameworks that enable professionals to prioritize ethical considerations in the design, development, and deployment of AI and autonomous systems (hereinafter referred to collectively as AI systems).

Data, especially that of consumers, is one of the most valuable commodities in our information-driven economy. The procurement and analysis of data represents a critical element for how firms of all sizes design their products, determine their target population, and constantly improve their offerings to better-serve customers. In a perfect world, consumers and firms have full information transparency and agree how information is obtained and used. Unfortunately, this is not the case, which justifies the existence of the Federal Trade Commission's (FTC) power to protect consumers against unfair or deceptive practices.

We applaud the FTC in its efforts to improve its rulemaking for the purpose of protecting consumers from harmful commercial surveillance and lax data security practices. Throughout our responses, IEEE-USA asserts that data about an individual belongs to that individual, in some cases, in a non-exclusive way. When a corporation collects, infers, or acquires an individual's data, that individual must be aware of their profile, what data is included, why the data is being held, and how it is being used. Overall, we advocate for complete transparency when AI systems procure, analyze, and utilize information for consequential and non-consequential decision-making. We hope that our input into this process complements how the FTC thinks about risks of AI systems under its jurisdiction.

Compilation of answers to selected questions:

1. Which practices do companies use to surveil consumers?

Internet and other communication-related platforms, applications, and devices routinely collect or infer health, financial, and biometric information without user knowledge, control, or consent. This includes data directly entered by users, acquired from third parties, or inferred by user activity/content. This data may be in the form of text/numbers, photographs/images, and behavior such as "hovering" over content/links, rate of keystrokes, search topics, GPS/Cellular/Wifi location triangulation, IP/MAC/SIM, and site identification, among other sources.

Data collected by an application is stored on a user's device in a cookie file or local browser storage. It can be transmitted to remote storage controlled by the application owner and forwarded by any number of intermediate systems including, but not limited to, the user's internet provider, a wireless access point, routers, gateways, and load balancers. Encrypted data may be decrypted and analyzed by an application provider who holds the key or an

approved authentication certificate. Each keystroke can be captured even before any explicit post, commit, or save button is pressed.

Internet and other communication-related platforms, applications, and devices regularly attempt to "fingerprint" or uniquely recognize users using a combination of seemingly innocuous attributes such as browser type and version, operating system, active plugins, time zone, language, screen resolution and more. When thwarted by users' attempts to avoid such fingerprinting, many sites have introduced increasingly aggressive and complicated fingerprinting mechanisms. One such example is "canvas fingerprinting" which goes to great lengths to attempt to fingerprint users usually without their knowledge and to overcome their attempts to evade simpler fingerprinting mechanisms.

Web trackers, a type of software commonly used to record users within and across websites – e.g., Google Analytics, Facebook Domain Insights, and "33 across" – are increasingly designed to report back to the manufacturer about the network activities of their users. It is increasingly difficult to find privacy preserving products for the home and small business market.

2. Which measures do companies use to protect consumer data?

Once data is within a company, it can be protected through encryption, access restrictions, audits, and policies such as anonymization. Users can gain transparency and agency about a company's data policies by having access to privacy agreements, and terms of use.

3. Which of these measures or practices are prevalent? Are some practices more prevalent in some sectors than in others?

Browser fingerprinting is prevalent. SimilarTech.com (https://www.similartech.com/categories/conversion-&-analytics) reports usage of web trackers across the top 10K websites, the top 100K website, the top one million websites and the entire Internet. They report that Google Analytics alone is used across 68.9 percent of the top 10K websites and 62 percent of the top one million websites.

4. How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?

Scale is one of the main factors for considering the effects of commercial surveillance on consumers. Today, firms of any size can directly or indirectly gather information on virtually any variable (demographic or otherwise) of their target population. A couple of decades ago, such an endeavor would have been prohibitively expensive. Advances in hardware and software, including artificial intelligence (AI) systems, have decreased the transaction costs needed to access up-to-date information on consumers, their revealed preferences, social networks, and any other imaginable behavior.

The systems built to gather consumer data are employed for a variety of tasks. Without limitations, microtargeting and behavioral advertising can enable manipulation outside a user's awareness and explicit control (e.g., delivering a suggestion for unhealthy food or addictive substances or conspiracy theories exactly when a person is vulnerable to them) for the purpose of exploiting, manipulating, and radicalizing others. Subtle-to-the-user practices also have consequential societal impacts. For example, voting misinformation and voting messaging - e.g., how "my friends" voted - sways elections. Alternatively, agreeing to the autoplay feature in YouTube can result in the radicalization of a subpopulation of viewers. The autoplay feature can be disabled, but it is automatically re-enabled if a user clicks on the page. Many pages are designed to trick users into clicking. Some ways this is done is via the inclusion of "hot spots" on the page with a graphic or image, filling the top of the page so the user needs to scroll (click) for content, and drawing the page in stages. This can cause the viewer to

accidentally click on a link that is different from their intended target. One way this occurs is when an individual wishes to click for more information, but the screen is redrawn so that an advertiser link appears on the same spot the more information link previously occupied.

The Accept Cookie prompt is a form of an opt-in mechanism prevalent in the design of commercial websites, but since it defaults to "All," is hard to read, includes multiple steps and pages, and could be misunderstood, it does not provide protection to consumers or represents a useful means of conveying how companies intend to use personal data.

5. Are there some harms that consumers may not easily discern or identify? Which are they?

In addition to the targeted manipulation of consumers, users are unaware that their personal data is collected with the purpose of displaying selective content in the form of ads, search results, and even specific web page options. This type of targeting may be sufficiently opaque that even system creators are unaware of discriminatory/abusing behavior taking place. Users can be targeted for manipulation and nudging outside their explicit awareness including when they are most vulnerable (e.g., an individual with bi-polar syndrome entering the manic phase and susceptible to certain advertising, a young girl with an eating disorder susceptible to diet products, a recover gambler susceptible to advertising for gambling, a citizen vulnerable to conspiracy theories, a patient diagnosed with an illness susceptible to medical misinformation). The same technology that enables businesses to zero in on a person interested in a niche consumer good can also target individuals with manipulative messaging to which they are uniquely vulnerable.

How data is managed by firms can lead to consumers experiencing reputational damage. Their information is accessible to different types of stakeholders from law enforcement agencies to criminal enterprises. This is enabled by how, in general, intellectual property ownership is automatically transferred to online service providers via opaque terms of use and boilerplate click-through agreements. This is strengthened by privacy policies and Terms of Service designed to protect firms and are usually very hard for consumers to understand. Even if companies claim to offer a way to opt-out, these alternatives can be implemented in a manner that is difficult or impossible to use in practice.

Opt-out forms frequently default to favoring a company's data collection activities with dire consequences if a user disagrees with these terms. In addition, the forms are inconsistent and may lead users to believe that they have opted-out because the On/Off or Accept/Continue settings are intentionally confusing. In some cases, such as Google Docs, it is only after reading several pages of the user agreement before it is revealed that the data is available to third parties. It also seems that a user's opt-out choice can be reset without their knowledge.

6. Are there some harms that consumers may not easily quantify or measure? Which are they?

Some harms are not easily quantified or measures. Most online consumers are unaware of the negative impact caused by the lack of privacy protection on the internet. They do not understand that the limited liability protections available to online service providers through Section 230 of the Communications Decency Act shield providers from legal challenges in ways not available to print, broadcast, and other forms of commercial media. Since anything posted on the internet – due to the distributed nature and replication provided – can never actually be withdrawn or destroyed, simply issuing a Cease-and-Desist request without punishment means that any offensive act can no longer be considered a "first-time violation." A proven harm could be considered a repeat offense as any content on the internet is automatically replicated and instantly distributed.

The detailed profiles that social media companies build for each of their users make advertising even more powerful by enabling advertisers to tailor their messages to individuals. These profiles often include the size and value of your home, what year you bought your car, whether you're expecting a child, and whether you buy a lot

of beer. Consequently, social media has a greater ability to expose people to ideas as fast as they individually will accept them. The same mechanisms that can recommend a niche consumer product to just the right person or suggest an addictive substance just when someone is most vulnerable can also suggest an extreme conspiracy theory just when a person is ready to consider it.

7. How should the Commission identify and evaluate these commercial surveillance harms or potential harms? On which evidence or measures should the Commission rely to substantiate its claims of harm or risk of harm?

Research into the possible use of broad statistical evaluation and/or large numbers of "dummy" users to identify the types of abuses is warranted. Some websites attempt to prevent such research with terms of service clauses. Legislation such as the DMCA or CFAA should not be used to shield web sites from research aimed at documenting and quantifying actual or potential harms.

Third party reviews and audits should be conducted, and the results made available for any online service with a membership of "reference number" of users or when annual revenue from online advertising or annual online retail sales exceeds "a reference annual income."

The Commission could seek quantifiable data on the number of users choosing privacy preserving technologies such as browser extensions, tracker blockers, VPNs, Tor, and others. Similarly, it could engage with companies who produce these privacy preserving technologies regarding the "game of escalation" they encounter to thwart increasingly invasive mechanisms.

10. Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?

The fact that data is publicly visible does not alter the need for personal control, or to restrict aggregation in some way. Data collected in public spaces may be exempt, but data collected from, about, and inferred about consumer online activities or biometrics, directly or indirectly, should be subject to regulated protection. Fundamentally, government policies should recognize that individuals own information collected or inferred about themselves. This should include browser fingerprinting technology - a method that websites use to collect information about your browser type and version, as well as your operating system, active plugins, time zone, language, screen resolution, and various other active settings - because it is important to recognize that even data that one might not consider personally identifiable when used in isolation can be used in combination with other data to uniquely identify individuals. All this information can be automatically added to the packet and available to the service.

It is especially notable that location data over time can uniquely identify most individuals. Collecting this information over a relatively short period of time (days) can reveal an individual's home and place of business, where they exercise, whether they seek regular medical treatment, where they worship, etc. Even the combination of home and work location can uniquely identify many people, even if not explicitly tagged with their name or other data that is more commonly considered personally identifiable.

11. Which, if any, commercial incentives and business models lead to lax data security measures or harmful commercial surveillance practices? Are some commercial incentives and business models more likely to protect consumers than others? On which checks, if any, do companies rely to ensure that they do not cause harm to consumers?

The objective of advertising is to change the thinking and/or behavior of consumers. Such impact is independent of the potential harm to society – historically promoting cigarette smoking is an example. Advertisers act on behalf of the product/service/action they promote, and some may have a disincentive to consider or respond to any ethical or other consideration of harm to the consumer.

The B2B data marketplace is one of the business models that can incentivize harmful commercial surveillance practices. Daily, consumers interact with products that aggregate information or allow third parties to do so. The lack of transparency and scrutiny by the public regarding how this information is stored, protected, or distributed provides opportunities for using this data in ways that may harm consumers. In other words, if consumers had complete visibility of how their information was commercialized, they may think twice before freely providing their emails, date of birth, or using services whose terms explicitly describe the way their interactions with a product will be used in a for-profit manner.

The platforms that develop the personal profiles and deliver the micro-targeted audience for these ads have a similar economic incentive but have alternative services/paying customers as alternatives. Unfortunately, increasingly comprehensive individual consumer profiles, facilitated by big data and analytics, real time monitoring of consumer behavior, and augmented by AI, have transformed advertising. It has gone from a world of focus and demographic groups to individual surveillance and monitored micro-targeting. This significant persuasion opportunity is one key to platform profitability.

Company brands and reputation depend on consumer trust. Setting clear rules and standards of behavior helps to assure a level playing field and healthy competition. Many consumers are willing to accept the use, sale, and collection of their most intimate personal details in exchange for the convenience and entertainment that online services provide. Putting transparency first, requesting consent, and following up on punishment for abuse and misuse will increase the sense of trust and encourage customer loyalty.

12. Lax data security measures and harmful commercial surveillance injure different kinds of consumers (e.g., young people, workers, franchisees, small businesses, women, victims of stalking or domestic violence, racial minorities, the elderly) in different sectors (e.g., health, finance, employment) or in different segments or "stacks" of the internet economy. For example, harms arising from data security breaches in finance or healthcare may be different from those concerning discriminatory advertising on social media which may be different from those involving education technology. How, if at all, should potential new trade regulation rules address harms to different consumers across different sectors? Which commercial surveillance practices, if any, are unlawful such that new trade regulation rules should set out clear limitations or prohibitions on them? To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?
b. To what extent do commercial surveillance practices or lax data security measures harm children, including teenagers?
13. The Commission here invites comment on commercial surveillance practices or lax data security measures that affect children, including teenagers. Are there practices or measures to which children or teenagers are particularly vulnerable or susceptible? For instance, are children and teenagers more likely than adults to be manipulated by practices designed to encourage the sharing of personal information?
16. Which sites or services, if any, implement child-protective measures or settings even if they do not direct their content to children and teenagers?
17. Do techniques that manipulate consumers into prolonging online activity (e.g., video autoplay, infinite or endless scroll, quantified public popularity) facilitate commercial surveillance of children and teenagers?
If so, how? In which circumstances, if any, are a company's use of those techniques on children and teenagers an unfair practice? For example, is it an unfair or deceptive practice when a company uses these

techniques despite evidence or research linking them to clinical depression, anxiety, eating disorders, or suicidal ideation among children and teenagers?
18. To what extent should trade regulation rules distinguish between different age groups among children (e.g., 13 to 15, 16 to 17, etc.)?

With respect to questions 12-18, IEEE USA has the following observations. IEEE-USA believes that privacy should be enforced broadly but there are special, well documented risks to minors. Organizations exist that specifically focus on research about potential harms to children and we encourage the Commission to incorporate the recommendations of these into your work. Privacy and the security of data and individuals is an appropriate concern for all sectors and age groups, but as indicated, the risks do vary for these. Organizations building individual profiles should be obligated to protect minors and address the reality that this community is at significant risk from self-harm and online abuse. The addictive factors that can affect all users apply here, as does the reinforcement of problematic interactions such as bullying, and the incentives to post/re-tweet outrageous or frightening content. These factors, along with behaviors encouraged in gaming environments may increase antisocial actions, depression, and isolation among young persons.

Legally mandated ages for consent, with confirmed parental consent as an alternative, should be required in many situations. Transparency with respect to potential abuses is needed to be able to fairly determine consent. Opt out from some risky environments should be available for persons above the age of consent as well. While many sites require birth year information as part of a registration process, analytics can also identify age related characteristics and should be used to minimize the impact on higher risk individuals. Organizations that use or ignore the personal data they obtain in their amplification/recommendation or algorithmic interactions with minors must be held accountable for adverse results.

Significant focus on protecting privacy and abuse of minors will improve protection of users in all sectors. Transparency, disclosure, user controls, notifications, and education – all starting from the premise of consumers having informed knowledge and ownership interest in the data about them is part of the solution.

30. Should the Commission pursue a Section 18 rulemaking on commercial surveillance and data security? To what extent are existing legal authorities and extralegal measures, including self- regulation, sufficient? To what extent, if at all, are self-regulatory principles effective?

35. Should the Commission take into account other laws at the state and federal level (e.g., COPPA) that already include data security requirements. If so, how? Should the Commission take into account other governments' requirements as to data security (e.g., GDPR). If so, how?

In response to questions 30 and 35, IEEE-USA supports strengthening federal laws and regulations to protect individual digital privacy and believes that Congress and regulatory agencies should adopt and implement laws, regulations, and processes that significantly increase the digital privacy protections of U.S. citizens.

The U.S. has fewer restrictions on the collection, use, and possible abuse of personal information than many other countries, including those in the European Union. The absence of a comprehensive federal data protection law is a missed opportunity for the U.S. to globally shape and address data rights, practices, and privacy. The current patchwork of federal and state laws lacks coherence and is insufficient. Consistency with GDPR and other existing laws and regulations would not only ensure that Americans are offered protections similar to those of EU citizens, but it would also make compliance easier for corporations which must navigate multiple regulatory environments. It could also lower the costs for both implementation and enforcement.

Self-regulatory principles are ineffective. Advances in information technologies and the ubiquitous presence of AI technologies have not only challenged our ability to protect individual privacy, they have also created situations

where U.S. citizens are largely unaware of the extent and scope to which their personal data is being collected, how it is being used, and who is applying that data to influence their or others' actions, resulting in increasing threats to Americans' digital privacy. Physical identification methods like facial recognition, voice recognition, "smart" devices, and electronic identifiers are used to track individuals. Digital sources, including online data collection, data analytics, compromised communications, and physical identification methods can be used to build a comprehensive picture of an individual. This understanding is then used to identify personal vulnerabilities, manipulate individuals, steal identities, and otherwise exploit or harm individuals, all with little or no disclosure of the collectors' intentions or identity.

IEEE-USA advocates for strong legal protection for individual privacy. Fundamentally, government policies must recognize that individuals own information collected or inferred about them.

36. To what extent, if at all, should the Commission require firms to certify that their data practices meet clear security standards? If so, who should set those standards, the FTC or a third-party entity?

To help protect both domestic and national security interests and the constitutional rights (speech and privacy) of users, baseline standards should be created for: verification procedures for account creation, when accounts can or should be removed or deactivated for a period, and when content can or should be removed or labeled with warning. Various organizations, including standards developing organizations such as IEEE, have relevant technical standards in the areas of technology ethics (https://standards.ieee.org/industry-connections/ec/), as well as security and data governance. Leveraging this work for specific regulatory guidance or to inform standards, guidelines, or best practices developed by NIST or the FTC can provide efficiencies. The time required to develop formal technical standards should be considered in terms of the interim impact of abusive practices that are occurring.

37. How do companies collect consumers' biometric information? What kinds of biometric information do companies collect? For what purposes do they collect and use it? Are consumers typically aware of that collection and use? What are the benefits and harms of these practices?

Biometric information collected from consumers includes facial scanning, iris scanning, fingerprints, gestures, voice recognition, gait analysis, and any additional characteristic which might distinguish one person from another or be linked to a specific individual. Consumers are rarely aware of this data collection (except when they are required to use it). Some of this data may reveal other information about a user such as gender, race, gender preference, age, or psychological characteristics (see the research of Michael Kosinski https://www.michalkosinski.com/research). Disclosure or use of some of these characteristics may be protected, or create highly prejudicial situations for employment, loans, housing, etc. These also bias algorithms in ways that are not transparent to users or system creators.

38. Should the Commission consider limiting commercial surveillance practices that use or facilitate the use of facial recognition, fingerprinting, or other biometric technologies? If so, how?

The public must be able to easily learn: the types of data being collected or inferred by any web service, device, or other electronic means; what data is retained and for how long; how it is used; and with which third parties it is shared, directly or indirectly. The same information must be available from those third parties.
All data collection mechanisms and devices must be disclosed to users, including web beacons, GPS location reporting, imaging/cameras, IoT device interactions, or other mechanisms for tracking user activity or data. Disclosed information must be sufficient for users to identify and invoke their privacy rights.

Each web service, or application must disclose ongoing content placed on the user's device and the uses of that content. This also applies to devices connecting to the Internet, or otherwise sharing data collected.

Communications, processing, or storage of data outside of the United States must be disclosed to users, even if data is not retained on the collecting device(s).

All these disclosures must be readily accessible and comprehensible to the average user without specialized knowledge,

53. How prevalent is algorithmic error? To what extent is algorithmic error inevitable? If it is inevitable, what are the benefits and costs of allowing companies to employ automated decision-making systems in critical areas, such as housing, credit, and employment? To what extent can companies mitigate algorithmic error in the absence of new trade regulation rules?
56. To what extent, if at all, should new rules require companies to take specific steps to prevent algorithmic errors? If so, which steps? To what extent, if at all, should the Commission require firms to evaluate and certify that their reliance on automated decision- making meets clear standards concerning accuracy, validity, reliability, or error? If so, how? Who should set those standards, the FTC or a third-party entity? Or should new rules require businesses to evaluate and certify that the accuracy, validity, or reliability of their commercial surveillance practices are in accordance with their own published business policies?

Questions 53 and 56 are answered together here. As AI systems are developed and deployed, the objectives of accuracy and lack of algorithmic bias towards marginalized or vulnerable groups may conflict, resulting in disparate impacts and lack of public confidence. To mitigate the negative impacts and encourage trustworthy AI, the objectives must be balanced by means that require clarity, transparency, and protection of all stakeholders. IEEE-USA believes that the FTC should establish rules that require companies to use existing metrics and standards. AI systems and their operators should, via federal regulatory activity, be required to comply with those existing standards for fairness, privacy, safety, and security.

Additionally, the FTC should establish transparency mechanisms for stakeholders. For example, require third-party access to data in standardized, machine-readable format, and create research investments into how the use of algorithms may disparately impact or disadvantage certain individuals and groups.

Like other systems that do so, AI systems must be evaluated throughout their lifecycle of design, implementation, and deployment. When these systems are deployed in critical applications such as employment, credit/finance, criminal justice, health systems, and allocation of public resources the FTC should require mechanisms for (and permit) independent verification and validation. Standards related to validity, reliability etc. are already being developed and adopted by standards development organizations like IEEE.

64. To what extent, if at all, does Section 230 of the Communications Act, 47 U.S.C. 230, bar the Commission from promulgating or enforcing rules concerning the ways in which companies use automated decision- making systems to, among other things, personalize services or deliver targeted advertisements?

Section 230 limits liability for online content providers/platforms including their amplification and selective presentation of content based on individual consumer profiles. While significant freedom should be permitted to consumers posting content (although perhaps not for foreign governments or others pretending to be consumers) the corporate or automated decision to promote this content to specific individuals should not be immune to regulatory or civil action.

74. In which circumstances, if any, is consumer consent likely to be effective?

Consent is only effective with fully available information, both public (types of data collected, application of this data, inferences created from this data) and personal (what data is collected, purchased, inferred, etc about the

individual consumer). Consumers need visibility and control over any personal information that a business may retain.

In addition, there is a need to find a balance between informed consent and information overload. Although consumers often click and agree to dozens of pages for a product's terms and conditions, this does not mean they understand what rights and obligations are assigned to their data. Further work is necessary to devise alternatives that properly inform the public of their data rights.

83. To what extent should the Commission consider rules that require companies to make information available about their commercial surveillance practices? What kinds of information should new trade regulation rules require companies to make available and in what form?

As we say in IEEE-USA position statements on the matter, the public must be able to easily learn: the types of data being collected or inferred by any web service, device, or other electronic means; what data is retained and for how long; how it is used; and with which third parties it is shared, directly or indirectly. The same information must be available from those third parties. All data collection mechanisms and devices must be disclosed to users, including web beacons, GPS location reporting, imaging/cameras, IoT device interactions or other mechanisms for tracking user activity or data. Disclosed information must be sufficient for users to identify and invoke their privacy rights. Each web service, or application must disclose ongoing content placed on the user's device and the uses of that content. This also applies to devices connecting to the Internet, or otherwise sharing data collected. Communications, processing, or storage of data outside of the United States must be disclosed to users, even if data is not retained on the collecting device(s). These disclosures must be readily accessible and comprehensible to the average user without specialized knowledge.

Disclosure for Users:

• For each web service or application, users must be able to obtain complete disclosure of information about them that is retained by the service, application, device or third party accessing the user's information – directly or indirectly.
• Similar disclosure and protections must also apply to third parties able to collect and retain personal data, including disclosure identifying all such third parties.

Control:

• Location and operational information from on-line devices may not be used for commercial purposes without explicit, informed user consent. Specific parameters affecting user contracts, pricing and liability must be provided to users prior to enabling such access.
• Users must be able to remove personally identifiable data about them easily from any site, cloud, or collection device.
• Users must be able easily to identify, terminate, delete and/or uninstall any content or applications placed on their devices or cloud.
• Disputes related to purging user data or applications must not default to licenses and arbitration processes that restrict the user's legal options.
• Users' consent for a device or web service to collect or infer data about them may not be interpreted to extend to information about their connections such as friends, contacts, or affiliates.
• A legally mandated age of consent must protect minors by restricting the collection and use of private information.
• The need to protect personal information collected must not prevent access needed to allow 3rd parties of the users choosing from access to the data needed to maintain and repair devices.
• Remote access to devices must be protected from abuses that might create physical risks or loss of information.

Notification:

• Users must be informed promptly and directly, if their private information is lost, compromised, or misused. Organizations collecting, inferring, or storing that information are responsible for the notification. Users must have the right to know the source of privacy violations and the responsible parties, whenever possible.
• Clear information must be available notifying recipients of paid advertising and content, along with a clear link to the source of that material and the intended beneficiary of the desired action for online content, available metadata should lead to sponsoring site(s), allowing the user to utilize the transparency and disclosure rights indicated above.

86. The Commission invites comment on the nature of the opacity of different forms of commercial surveillance practices. On which technological or legal mechanisms do companies rely to shield their commercial surveillance practices from public scrutiny?

Intellectual property protections, including trade secrets, for example, limit the involuntary public disclosure of the assets on which companies rely to deliver products, services, content, or advertisements. How should the Commission address, if at all, these potential limitations?

An individual's personal data should be protected, but not from access and control by that individual.

87. To what extent should the Commission rely on third-party intermediaries (e.g., government officials, journalists, academics, or auditors) to help facilitate new disclosure rules?

see response to #83 above

89. To what extent should trade regulation rules, if at all, require companies to explain (1) the data they use, (2) how they collect, retain, disclose, or transfer that data, (3) how they choose to implement any given automated decision-making system or process to analyze or process the data, including the consideration of alternative methods, (4) how they process or use that data to reach a decision, (5) whether they rely on a third-party vendor to make such decisions, (6) the impacts of their commercial surveillance practices, including disparities or other distributional outcomes among consumers, and (7) risk mitigation measures to address potential consumer harms?

see response to #83 above

90. Disclosures such as these might not be comprehensible to many audiences. Should new rules, if promulgated, require plain-spoken explanations? How effective could such explanations be, no matter how plain? To what extent, if at all, should new rules detail such requirements?

see response to #83 above

Personal data about an individual should be protected, but not from access and control by that individual.

94. How should the FTC's authority to implement remedies under the Act determine the form or substance of any potential new trade regulation rules on commercial surveillance? Should new rules enumerate specific forms of relief or damages that are not explicit in the FTC Act but that are within the Commission's authority? For example, should a potential new trade regulation rule on commercial surveillance explicitly identify algorithmic disgorgement, a remedy that forbids companies from profiting from unlawful practices related to their use of automated systems, as a potential remedy? Which, if any,

other remedial tools should new trade regulation rules on commercial surveillance explicitly identify? Is there a limit to the Commission's authority to implement remedies by regulation?

The best protections will be preventative, combining user education as well as supplier transparency, disclosure, and application of standards/regulatory guidelines. Regulations should require that all companies offer a truly privacy preserving option that maintains all features possible and is audited for privacy compliance and available for a reasonable level of price increase.

When systems make life-impacting or consequential decisions, preserving privacy, equity, and justice requires that individuals be informed about, and permitted to, question decisions and have access to systems that enable redress. To improve the status quo in this respect, policymakers should consider:

- Defining pathways for all stakeholders to report problems, question results, provide additional information relevant to automated decision making, and receive redress when they are harmed.
- Defining pathways for individuals to review, verify and question input data about them as individuals.

95. The Commission is alert to the potential obsolescence of any rulemaking. As important as targeted advertising is to today's internet economy, for example, it is possible that its role may wane. Companies and other stakeholders are exploring new business models. Such changes would have notable collateral consequences for companies that have come to rely on the third-party advertising model, including and especially news publishing. These developments in online advertising marketplace are just one example. How should the Commission account for changes in business models in advertising as well as other commercial surveillance practices?

It is critical that regulation start with the basic principles such as the individual's right to ownership of all personal data collected, acquired, inferred, and information about how it is being used, and who has access to that data as well as who is paying for the use of the data. By establishing basic principles, the application of the regulations should be more straightforward and have a longer applicability as technology evolves.

==========

Relevant IEEE-USA position statements are attached below and can be found at the following links:

1) Digital Personal Privacy, Awareness, and Control: https://ieeeusa.org/assets/public-policy/positions/communications/DigitalPrivacy1121.pdf
2) Democratic Use of Artificial Intelligence: https://ieeeusa.org/assets/public-policy/positions/ai/Democratic_Use_of_AI_1121.pdf
3) Privacy, Equity, and Justice in Artificial Intelligence: https://ieeeusa.org/assets/public-policy/positions/ai/Privacy_Equity_Justice_1121.pdf

IEEE★USA

POSITION STATEMENT

Digital Personal Privacy, Awareness, and Control

Adopted by the IEEE-USA Board of Directors November 4, 2021

IEEE-USA supports greatly strengthening laws and regulations protecting individual digital privacy in this era of big data, analytics, and artificial intelligence. The U.S. has fewer restrictions on the collection, use, and possible abuse of personal information than many other countries, including those in the European Union. Advances in information technologies have created situations where U.S. citizens are largely unaware of the extent and scope to which their personal data is being collected, how it is being used, and who is applying that data to influence their, or others', actions. Congress and regulatory agencies should adopt and implement laws, regulations, and processes that significantly increase the digital privacy protections of U.S. citizens.

Threats to Americans' digital privacy abound. Physical identification methods like facial recognition, voice recognition, "smart" devices, and electronic identifiers are used to track individuals. Digital sources, including online data collection, data analytics, compromised communications, and physical identification methods can be used to build a comprehensive picture of an individual. This understanding is then used to identify personal vulnerabilities, manipulate individuals, steal identities, and otherwise exploit or harm individuals, all with little or no disclosure of the collectors' intentions or identity.

IEEE-USA advocates for strong legal protection for individual privacy. Fundamentally, Government policies must recognize that individuals own information collected or inferred about them. Examples of specific areas where increased protections are needed include:

IEEE-USA | 2001 L Street, N.W., Suite 700, Washington, D.C. 20036-4928 USA
Office: +1 202 785 0017 | Fax: +1 202 785 0835 | E-mail: ieeeusa@ieee.org | Web: https://www.ieeeusa.org

Public Transparency:

- The public must be able to easily learn: the types of data being collected or inferred by any web service, device or other electronic means; what data is retained and for how long; how it is used; and with which third parties it is shared, directly or indirectly. The same information must be available from those third parties.
- All data collection mechanisms and devices must be disclosed to users, including web beacons, GPS location reporting, imaging/cameras, IoT device interactions or other mechanisms for tracking user activity or data. Disclosed information must be sufficient for users to identify and invoke their privacy rights.
- Each web service, or application must disclose ongoing content placed on the user's device and the uses of that content. This also applies to devices connecting to the Internet, or otherwise sharing data collected. Communications, processing or storage of data outside of the United States must be disclosed to users, even if data is not retained on the collecting device(s).
- These disclosures must be readily accessible and comprehensible to the average user without specialized knowledge.

Disclosure for Users:

- For each web service or application, users must be able to obtain complete disclosure of information about them that is retained by the service, application, device or third party accessing the user's information – directly or indirectly.
- Similar disclosure and protections must also apply to third parties able to collect and retain personal data, including disclosure identifying all such third parties.

Control:

- Location and operational information from on-line devices may not be used for commercial purposes without explicit, informed user consent. Specific parameters affecting user contracts, pricing and liability must be provided to users prior to enabling such access.
- Users must be able to remove personally identifiable data about them easily from any site, cloud or collection device.
- Users must be able easily to identify, terminate, delete and/or uninstall any content or applications placed on their devices or cloud.
- Disputes related to purging user data or applications must not default to licenses and arbitration processes that restrict the user's legal options.
- Users' consent for a device or web service to collect or infer data about them may not be interpreted to extend to information about their connections such as friends, contacts or affiliates.
- A legally mandated age of consent must protect minors by restricting the collection and use of private information.

- The need to protect personal information collected must not prevent access needed to allow 3rd parties of the users choosing from access to the data needed to maintain and repair devices.
- Remote access to devices must be protected from abuses that might create physical risks or loss of information.

Notification:

- Users must be informed promptly and directly, if their private information is lost, compromised, or misused. Organizations collecting, inferring or storing that information are responsible for the notification.
  Users must have the right to know the source of privacy violations and the responsible parties, whenever possible.
- Clear information must be available notifying recipients of paid advertising and content, along with a clear link to the source of that material and the intended beneficiary of the desired action.
  For online content, available metadata should lead to sponsoring site(s), allowing the user to utilize the transparency and disclosure rights indicated above.

This statement was developed by the IEEE-USA Committee on Communications Policy and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public policy interests of the over 150,000 engineering, computing and allied professionals who are U.S. members of the IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.

IEEE-USA

POSITION STATEMENT

Democratic Use of Artificial Intelligence

Adopted by the IEEE-USA
Board of Directors (November 2021)

IEEE-USA believes that AI systems can increase quality of life, improve government efficiency, and promote societal well-being. However, when used improperly or by malicious actors, AI systems can jeopardize human rights, violate the U.S. Constitution, create and amplify harmful mis- and disinformation, and pose severe threats to individual and collective privacy. US government action and collaboration with like-minded states can help ensure that AI systems promote rather than threaten democratic values. IEEE-USA recommends that the U.S. government:

1. **Encourage international standards, diplomacy, and agreements to uphold human rights, promote innovation and commerce, and govern AI systems and techniques.**[1] While there has been considerable progress in declarations on the ethical use of AI systems by governments, corporations, and international organizations, there is a need for an overall framework that links national and global efforts to address the use of AI in ways that support democracy. We recommend that the U.S. government:

    - Lead the development of such a framework as well as promote its use and further development among allies and like-minded nations. This can be achieved through:
        - Existing and evolving standards;
        - Diplomatic efforts;
        - Strong domestic and international intellectual property policy; and,
        - Strengthening both domestic and international agreements on the ethical uses of AI systems; as well as how data is collected, used, and retired; and,
    - Undertake and promote collaboration with companies, academics, and stakeholders in relevant technical and social scientific fields within the context of this common framework.

2. **Promote transparency, human agency, and accountability in AI systems to reduce the promotion of extremism, misinformation, and disinformation.** The AI systems that drive content recommendation systems used by online platforms can

[1] See the IEEE-USA position statement on "Accelerating Inclusive AI Innovation by Building Trust," https://ieeeusa.org/wp-content/uploads/2021/03/AIPC_BuildingTrustInAI.pdf.

create echo chambers that are harmful to society. To mitigate the harmful impacts of these systems, we recommend that the U.S. government:

- Establish clear transparency standards that allow users to understand why they were shown certain content, particularly when it may be the result of commercial or foreign entities;
- Invest in increasing technical literacy to improve public understanding of personal information that AI systems may infer about them, and how these systems could influence their thinking; and,
- Partner with allies and like-minded nations to establish transparent ethical guidelines for the use and accountability of AI systems that could manipulate individuals or influence public opinion so that the public can understand who is attempting to influence them and how they are doing it.

3. **Support human rights and democratic governance of AI through the rule of law and the right to privacy.** To encourage the development and implementation of AI systems that respect and further human rights, we recommend that the U.S. government:

- Establish principles for the design and operational use of AI systems to prevent violations of human rights and the U.S. Constitution;
- Create, where possible, accountability mechanisms for groups deploying AI systems that have the potential to violate human rights principles or the U.S. Constitution;
- Require the disclosure of when AI and automated decision systems are used, and how their use may impact users; and,
- Increase investments in research on the human rights impacts of AI systems.

To ensure that AI systems used by popular online platforms promote democracy, we recommend that the U.S. government:

- Create partnerships between government, industry, and academia to monitor the spread and impacts of mis- and disinformation, extremist content, and foreign malign influence on internet platforms, subject to appropriate legal and constitutional limitations; and,
- Place restrictions on the personal data that foreign-operated internet platforms can collect about U.S. users, preventing anti-democratic actors from performing sophisticated microtargeting of propaganda.

To promote the democratic governance of AI systems,[2] we recommend that the U.S. government:

- Increase investment in public education about potential impacts of AI (including both its capabilities and limitations); and,
- Develop mechanisms for soliciting broad public input on the governance of AI, particularly from marginalized or vulnerable communities.

[2] See also the IEEE-USA position statement on "Effective Governance of AI."

4. **Protect intellectual property (IP) from manipulation including theft, excessive patent filing, and abuse caused by incorporating patented technology into international standards.** IP policy should be recognized as a national priority with special commitment to IP policy enhancement around AI-related emerging technologies. We recommend that the U.S. government:

    - Combat any actions that would directly or indirectly negatively influence international standards settings;
    - Combat the injection of a large body of low-quality prior art that would adversely impact the United States Patent and Trademark Office; and,
    - Continue and expand efforts to counter and sanction the foreign theft of intellectual property through hacking, espionage, blackmail, and illicit technology transfer.

5. **Clarify the lines between free speech and censorship in content moderation.** Internet platforms use AI systems to select, target, and promote content. These systems often amplify content that many consider to be false or manipulative. Given the exponentially increasing quantity of content and lack of knowledge of speaker identity, individuals using these platforms are disadvantaged in verifying the accuracy of content and sources. However, actions and mechanisms to rectify these problems must be carefully balanced with the freedom of expression. Without affecting individuals' right to freedom of expression, we recommend that the U.S. government:

    - Establish guidelines for transparent content moderation policies that limit:
        - the ability to create fake accounts to promote or amplify messages at large scale;
        - the ability to spread artificially generated harmful audio, video or photographic material that appropriate or mimic real people without consent ("deepfakes"); and
        - the ability to spread messages that are factually incorrect or carefully crafted to manipulate and mislead;
    - Establish guidelines clarifying content moderator's rights and responsibilities for regulating speech that balance openness, transparency, and free speech with platforms' right to control their products.
    - Require that AI systems, which are limited in their ability to accurately and transparently detect harmful content, not be exclusively relied upon for content moderation;
    - Require that internet platforms provide, subject to appropriate privacy restrictions, the data necessary for researchers and the public to independently evaluate the extent of possible manipulation or abuse; and,
    - Scale guidelines for accounts and platforms so that they increase with the size of their audiences and reach.

This statement was developed by IEEE-USA's Artificial Intelligence Policy Committee and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public policy interests of the nearly 150,000 engineering, computing and allied professionals who are U.S. members of IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.

IEEE★USA

POSITION STATEMENT

Privacy, Equity, and Justice in Artificial Intelligence

Adopted by the IEEE-USA
Board of Directors (November 2021)

AI's ubiquitous presence in society has challenged our ability to protect privacy and ensure equity and justice. The foundational principles below provide a legal, technical, and policy framework to address these challenges going forward and resolve problems embedded in existing AI uses and systems, such as when AI systems are trained with past data embedded with patterns of inequality and human bias. Building this framework requires updating, harmonizing, and streamlining federal laws, policies, and guidelines as follows:

1. Data ownership, data rights, and privacy

Equitable AI practices require a clear legislative framework for data ownership, confidentiality of data, and rights of access to data used in and by AI systems--essential to protecting privacy and autonomy. Moreover, *the absence of a comprehensive data protection law at the federal level in the U.S. is a missed opportunity for the U.S. to globally shape and address data rights, practices, and privacy.* The current patchwork of federal and state laws lacks coherence and is insufficient.[1]

- ***Enact clear and comprehensive data protection law(s) at the federal level*** Internet and other communication-related platforms, apps, and devices routinely collect or infer health, financial, and biometric information without user knowledge, control, or consent. The U.S. sectoral approach to data regulation leaves vast swaths of individuals' intimate data unprotected and fails to provide a clear framework of permissible operation for AI

[1] Our current federal and state patchwork of data laws lends to confusion and inefficiencies and precludes the U.S. from shaping private and government sector data practices on a national and international level. At the federal level, there is a sectoral-based approach to data regulation by both public and private sectors (e.g., health – Health Insurance Portability and Accountability Act; and financial – Gramm-Leach-Bliley Act). Given current data collection practices (communication platforms, apps, and devices routinely collect health, financial, and biometric data, and PII), the existing sectoral approach leaves vast swaths of individuals' intimate data unprotected in the current federal legislative scheme. At the state level, all 50 states have passed varying forms of data breach laws and a myriad of states have enacted comprehensive data regulation and biometric laws, such as the California Consumer Privacy Act (CCPA) and the Illinois Biometric Information Privacy Act. California, via CCPA, and the European Union's General Data Protection Regulation Act (GDPR) both provide legislative frameworks that have altered private sector data practices on a global scale.

systems and their operators, leading to inefficiencies and confusion. Comprehensive data regulation through legislative action should incorporate principles like Fair Information Practice Principles (FIPPs) that:

- **Establish data collection and data use limitations, data quality standards, and security safeguards.**
- **Require clearer notice of data collection practices with truly effective opportunities to consent (or not) to such data collection.**
- **Mandate transparency and user control in use of individual data.** Consumers are often unaware of how their data is collected and used; long, complex Terms of Use and privacy policies obscure actual data practices. Mandate that users have the right to access, review, store, and delete personal user data, including behavioral data used for tracking and AI recommendation systems, and require an option to opt-out of tracking.

2. Mitigate disparate impacts of AI

When AI systems are developed and deployed, objectives of accuracy and lack of algorithmic bias towards marginalized or vulnerable groups can conflict, resulting in disparate impacts and lack of public confidence. To mitigate, objectives must be balanced by means that require clarity, transparency, and protection of all stakeholders.

- ***Establish and mandate metrics and standards.*** AI systems and their operators must comply with standards for fairness, privacy, safety, and security.
- ***Establish transparency mechanisms for stakeholders.*** For example, require third-party access to data in standardized, machine-readable format.
- ***Create research investments on how the use of algorithms may disparately impact or disadvantage certain individuals and groups.***

3. Ongoing verification and validation of AI systems

Increasingly, AI systems directly impact human life, individual rights and societal well-being and, like other systems that do so, must be evaluated throughout their lifecycle, i.e., design, implementation, and deployment. When AI systems are deployed in critical applications such as employment, credit/finance, criminal justice, health systems, and allocation of public resources:

- ***Require transparency about the training data and other developmental inputs.***
- ***Require mechanisms for (and permit) independent verification and validation.***

4. Redress

When AI systems make life-impacting decisions, preserving privacy, equity, and justice requires that individuals be informed about, and permitted to, question decisions and have access to systems that enable redress.

- **Define pathways for all stakeholders to report problems, question results, provide additional information relevant to automated decision making, and receive redress when they are harmed.**
- **Define pathways for individuals to review, verify and question input data about them as individuals.**

- **Require human teams be tasked to investigate errors with clear pathways for stakeholders to communicate with teams and require timely response.**
- **Require systems to produce explanations of their output that can be examined by human decision makers and other stakeholders.**
- **Provide clear statutory culpability and means of civil redress for entities in the AI supply chain responsible for harm to individuals, groups, or the environment.**

5. Baseline Standards for Platform Governance

AI systems are ubiquitous, and access to and use of online platforms is a requirement to be an effective citizen of the modern world (education, taxes, banking - all require online participation with platforms, devices, and apps that operate with and rely upon AI systems). **To protect both domestic and national security interests and the constitutional rights (speech and privacy) of users**, baseline standards should be created for: verification procedures for account creation; when accounts can or should be removed or deactivated for a period of time; and when content can or should be removed or labeled with warnings

6. Anti-Manipulation

When AI systems are built with detailed, fine-grained information about individuals, they can use this information to deliver customized suggestions to individuals. Without limitations, microtargeting and behavioral advertising can permit and enable manipulation outside a user's awareness and explicit control (e.g., *delivering a suggestion* for unhealthy food or addictive substances or conspiracy theories *exactly when a person is vulnerable to them*), thus, enabling systems or human operators to exploit, manipulate, and radicalize others. *Subtle-to-the-user practices have huge societal impacts*, e.g., voting misinformation and voting messaging (how "my friends" voted) sways elections; having an autoplay feature in YouTube (enables seamless radicalization of viewers). Legislation to mitigate such effects would:

- ***Require clear information about why a suggestion is being offered to an individual and about who is paying to deliver that suggestion.***
- ***Require disclosure of actor*** (human or AI) with whom the user is interacting.
- ***Require proactive steps to prevent harmful manipulation and abuse.***
- ***Require data and access necessary for independent research/evaluations of anti-manipulation measures.***
- ***Require verified identity for entities/persons paying for content or ad distribution.***

This statement was developed by IEEE-USA's Artificial Intelligence Policy Committee and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public policy interests of the nearly 150,000 engineering, computing and allied professionals who are U.S. members of IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.