Comments for FTC Hearing #12
"The FTC's Approach to Consumer Privacy."
Constitution Center
400 7th St, NW
Washington, DC 20024

30 May 2019

The following responses were developed by members of the IEEE-USA representing nearly 180,000 individual technology professionals in the United States. Our members are the men and women responsible for creating, deploying and using advanced electro technologies, including those that make up the internet. We do not speak for any specific company or technology. Rather, our members are technical experts who are concerned about the declining utility of the internet for many Americans and the rising risks to privacy posed by new technologies and practices.

We applaud the FTC for tackling this important issue. Digital privacy is one of the defining issues of our times. The internet has assumed a central place in American society. This is, overall, a very good thing for most Americans. However, the growing power of the internet has created opportunities that put individual internet users' at risk. American citizens have a right to privacy, and that right should not be taken away simply because they downloaded an app or visited a website.

The FTC has an opportunity to create the ground rules for conduct on the internet. Your efforts to establish these rules are needed and welcomed by American's technology professionals.

The questions below are those from the FTC hearings announcement: https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019?utm_source=govdelivery

- What are the actual and potential benefits for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these benefits?
    - Personalization of content allows companies to present "best fit" products that match the needs and wants of specific customers. This can make a customer's experience with that business more efficient. Personalized data can also allow companies to identify needs that a customer doesn't realize they have, or to foresee needs that are about to develop. Pampers, for example, could tell when a woman is pregnant and send her diaper coupons shortly before her child arrives
- What are the actual and potential risks for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these risks?
    - Companies collect massive amounts of personal data both explicitly (by consumer entry or actions) and by inferring data through the use of deep learning algorithms that can translate explicit disclosures into undisclosed personal information. This information can include personality profiles[i], sexual orientation,[ii] political leanings and a host of other characteristics that the individual may not want to become public. When you add shopping habits from loyalty cards, voter information, property records, magazine subscriptions and other data points, companies can construct a highly-detailed profiles of individuals -- with limited, if any, awareness by consumers.
    - Armed with this data, companies and other actors can produce highly persuasive content[iii] on every web page visited by that individual that allows tracking and/or paid content insertion. Within the foreseeable future it will be possible to insert deep-fake content continuously adjusted to maximize

user engagement and response. Fear and outrage are among the most effective engagement mechanisms, and fake content has been demonstrated to propagate much faster than valid information. These risks are real, they are pervasive on today's Internet, and consumers are encountering these at every "click", from simple marketing campaigns to terrorist recruiting or political propaganda. The "personalization" has moved from a benefit to a serious challenge to consumer informed choice and freedom of action without undue influence.

- The use of "big data" in automated decision-making has generated considerable discussion among privacy stakeholders. Do risks of information collection, sharing, aggregation, and use include risks related to potential biases in algorithms? Do they include risks related to use of information in risk scoring, differential pricing, and other individualized marketing practices? Should consideration of such risks depend on the accuracy of the underlying predictions? Do such risks differ when data is being collected and analyzed by a computer rather than a human?
    - Big data, in combination with AI-powered analytics, definitely create significant opportunities for bias and interaction inequality. Automated evaluation inevitably incorporates the biases of the creators and the culture in which it operates. In theory, algorithms could be "color blind", but big data includes thousands of proxies for race, nationality, sexual orientation, gender, and age that may be explicitly or implicitly used in personalizing marketing. A totally opaque "Sift" score[iv] is calculated for every online user. These can result in different pricing, levels of service or even what products are offered, including housing, jobs or other transactions where discrimination is prohibited by federal law. Discrimination in AI systems can, in some cases, be more damaging that non-digital discrimination because AI systems are so fast, so opaque, and so ubiquitous.
    - Discriminatory algorithms can be created unintentionally by using neutral decision criteria that result in biased results. But those algorithms can also be intentionally discriminatory.
- Should privacy protections depend on the sensitivity of data? If so, what data is sensitive and why? What data is not sensitive and why not?
    - It is unclear in the era of big-data analytics what data can be assumed to be "non-sensitive." The inference capabilities of AI systems permit virtually any "digital footprint" of the user to disclose information that would qualify as sensitive. Images from public cameras, for example, can be used to infer a tremendous amount of information about people in those photographs. While some data is especially sensitive and needs extra protection, such as medical records and financial information, all digital information needs protecting if individuals are to enjoy meaningful on-line privacy rights.
- Should privacy protection depend on, or allow for, consumer variation in privacy preferences? Why or why not? What are the appropriate tradeoffs to consider? If desired, how should this flexibility be implemented?
    - Every on-line consumer should be able to expect a certain level of privacy, and that privacy should not be negotiable. User ownership of their personal data must be the starting point for privacy protection, including explicit data provided by the user, tracking data collected about the user, inference data, as well as data provided by third parties and shared or aggregated data. Without comprehensive protection as well as transparency associated with use of data, users will be subject to micro-targeted persuasion affecting their ability to act as informed consumers, voters and citizens. Protections must primarily be based on informed opt-in agreements that are easy to understand. Abuse of protections requires significant financial and possible felony incarceration. Beyond these basic rights and protections, and armed with adequate information to understand how their data is being used, most consumers should be allowed to trade additional privacy for access, preferential rates, or whatever other incentives companies care to offer on an informed basis.

- Some on-line customers, especially children, will require greater non-revocable privacy rights, as they cannot provide informed consent.
- IEEE has a related standard project[v], IEEE P7012 Standard for Machine Readable Personal Privacy Terms, to facilitate this process.

- Market-based injuries can be objectively measured—for example, credit card fraud and medical identity theft often impact consumers' finances in a directly measurable way. Alternatively, a "non-market" injury, such as the embarrassment that comes from a breach of sensitive health information, cannot be objectively measured, because there is no functioning market for it. Many significant privacy violations involve both market and non-market actors, sources, and harms. Should the Commission's privacy enforcement and policy work be limited to market-based harms? Why or why not?
  - Market based considerations are not sufficient. Loss of one's credit card number may cost a family their savings, but the loss of one's on-line privacy can cost reputations, jobs, and respect. Not considering non-market injuries would be irresponsible.
  - It is worth noting that non-market injuries, such as reputational harm and emotional distress, can be quantified by the courts and are often part of judgments in lawsuits.
- In general, privacy interventions could be implemented at many different points in the process of collecting, processing, and using data. For example, certain collections could be banned, certain uses could be opt-in only, or certain types of processing could trigger disclosure requirements. Where should interventions be focused? What interventions are appropriate?
  - Privacy protections must be implemented at the very beginning of digital interactions, and they must be obvious, clear and should escalate as more data is requested. For example, if a website gathers information on an individual the moment they access the site, this fact must be conveyed to the individual BEFORE any data is collected. If, later in their session, the individual buys a product from the website, additional information must be provided detailing how this new data will be used. If the user uploads a selfie to the website, they need to be told how the website will use their photo, with whom it will be shared, and what data will be gleaned from it – all before the upload is completed. One ambiguous statement on the home page next to an opt-in box is insufficient.
  - Protections must be put in place to ensure that individuals who cannot voluntarily give up their privacy rights (especially children) cannot surrender their rights.
- Should policymakers and other stakeholders attempt to improve accountability for privacy issues within organizations? Why or why not? If so, how? Should privacy risk assessments be mandated for certain companies? Should minimum standards in privacy protections be required?
  - Just as organizations are responsible for handling credit card and health information correctly, organizations that collect digital information need to be accountable for how they handle that information. If companies want to collect data from customers, they must take responsibility for protecting that data and face legal consequences if they don't. Minimum privacy standards should be set and required for all companies collecting, processing and using private data.
  - A series of voluntary standards activities have been initiated and are in various states of completion via the IEEE Standards Association -- see https://ethicsstandards.org/p7000/ for the list. Key standard projects that warrant federal[vi] and industry participation include:
    - IEEE P7002 Data Privacy Process
    - IEEE P7003 Algorithmic Bias Considerations
    - IEEE P7004 Standard on Child and Student Data Governance

        - IEEE P7005 Standard on Employer Data Governance
        - IEEE P7006 Standard on Personal Data AI Agent Working Group
        - IEEE P7008 Standard for Ethically Driven Nudging for Robotic, Intelligent & Autonomous Systems
        - IEEE P7011 Standard for the Process of Identifying & Rating the Trust-worthiness of News Sources
        - IEEE P7012 Standard for Machine Readable Personal Privacy Terms
        - IEEE P7013 Inclusion and Application Standards for Automated Facial Analysis Technology

- How can firms that interface directly with consumers foster accountability of third parties to whom they transfer consumer data?
    - From the FTC's perspective, it is sufficient that companies must hold third parties accountable for handling individuals' private data. Companies that choose to collect private data are responsible for that data, even after it is transferred to a third party. If the collecting company is unsure of the integrity of the third parties with which it does business, then the collecting company should find another company to do business with. Contracts, along with strongly enforced federal protections and international cooperation should be used to enforce this rule.
- What are the effects, if any, on competition and innovation from privacy interventions, including from policies such as data minimization, privacy by design, and other principles that the Commission has recommended?
    - These policies will impact some of the business models, mostly those based on selling micro-targeted access to individuals based on highly invasive personal data profiles, but they will also open up innovation for new services that develop more consumer-friendly business models and potential for competition in markets where there now are entrenched dominate players.
    - Moreover, properly calibrated and enforced privacy protections will create a safer ecosystem for consumers, encouraging more on-line activity. Just as safe streets encourage shoppers to venture out at night, resulting in greater sales, so will enforceable privacy rights encourage customers to venture on-line in new ways. This will reward responsible companies and encourage new digital innovation.
- Do firms incur opportunity costs as a result of increased investments in privacy tools? If so, what are the tradeoffs between functionality, innovation, and security and privacy protections at the design level?
    - Designing in security, privacy and other protections should be a basic cost of doing business for an ethically oriented firm. Unfortunately, not all players are ethical. Within the current environment, ethical organizations are at a disadvantage because they must bear the costs associated with protecting users' privacy while unethical firms do not. Much like the lack of building codes encourages construction companies to cut corners – because all their competitors do – so to the lack of privacy rights encourages the abuse of digital information. Enforceable privacy rights, like building codes, reward ethical actors.
    - Privacy standards should establish a minimum level of privacy protection that must be built into any product or service. This is will have a cost, but it is a necessary cost to do business in our digital world. These standards should be set in a way that encourages innovation, experimentation and growth, while still protecting customers. There are also costs to not setting enforceable standards. Declining trust and rising risk could drive customers away from digital businesses and do harm to our society.
- If businesses offer consumers choices with respect to privacy protections, can consumers be provided the right balance of information, i.e., enough to inform the choice, but not so much that it overwhelms the decision maker? What is the best way to strike that balance and assess its efficacy?
    - Yes, but only up to a point. The complexity of privacy decision making in the world of big data and AI driven analytics will be difficult for all, and impossible for some, customers to understand. This is why

minimum standards are necessary to protect customers. Beyond these minimum standards, efforts must be made to articulate the opportunities and risks involved in giving up privacy. Simple statements letting customers know what they are giving up and why should be sufficient in most cases. Children, naturally, will require special protection since they cannot be expected to understand the implications of their decisions.

- To what extent do companies compete on privacy? How do they compete? To what extent are these competitive dynamics dictated or influenced by consumer preferences, regulatory requirements, or other factors?
    - If we allowed car companies to compete freely on safety, only Volvos (which explicitly marketed cars based on their safety) would have seatbelts. Recently, Apple has started ad campaigns based on superior privacy. European and California privacy legislation have also triggered industry responses -- either to provide new protections or to lobby for regulatory changes, providing consumers with some differentiation. While these limited efforts should be applauded, customers usually lack a proper understanding of the risks involved with their actions to evaluate the implications of their decisions, which is why the government set minimum levels of safety for cars, buildings, boats, electronics, and just about every other product on the market. On-line companies should be treated similarly with respect to customer privacy.
- Some academic studies have highlighted differences between consumers' stated preferences on privacy and their "revealed" preferences, as demonstrated by specific behaviors. What are the explanations for the differences?
    - Consumers are likely very unaware of the level of personal data being acquired and used, and of the risks these activities entail. For example, individuals may be unaware that sexual orientation is discernible by online photos,[ii] or other inferred characteristics that can affect their employment, Sift score, or other applications. Without having aware consumers operating in a transparent market, the mismatch between customer preferences and actions will persist. Furthermore, the virtual monopolies that a few companies enjoy effectively prevent consumers from exercising their privacy preferences. The uniquely intimate nature of the internet may also give customers a false sense of security when using it.
- Given rapidly evolving technology and risks, can concrete, regulated technological requirements – such as data de-identification – help sustainably manage risks to consumers? When is data de-identified? Given the evolution of technology, is the definition of de-identified data from the FTC's 2012 Privacy Report workable? If not, are there alternatives?
    - AI has improved remarkably since 2012. The confidence that a customer might have had in 2012 in his/her anonymity may no longer be valid in 2018 (see papers ii & iii in footnotes), and will be different in 2020, 2024 etc. This is one reason that regulations should focus on fiduciary and legal responsibilities, not specific technologies or algorithms. In other words, defining what information may not be gathered and what types of data may not be inferred is more useful than defining what types of technologies may be used to do analyses. Also, ongoing industry-consumer communication is needed to keep stakeholders aware of the most recent capabilities for analytical re-identification.
- What should the role of the Commission be in the privacy area? What would define successful Commission intervention? How can the Commission measure success?
    - The Commission needs to play a leading role in establishing minimum privacy rights and norms of behavior. The Commission needs to lead efforts to inform the public about their rights and the risks of

relinquishing their privacy. And the Commission needs to encourage industry participation in efforts to develop privacy standards.

Questions About Legal Frameworks

- What are the tradeoffs between ex ante regulatory and ex post enforcement approaches to privacy protection?
    - Ideally, ex ante regulatory actions and an established fiduciary obligation that companies protect their customers' personal data would be all that are needed, but that is unlikely to be the case. Given the speed at which technology is moving and the number of bad actors already operating in cyberspace, aggressive enforcement of privacy laws will likely also be required.
- The U.S. has a number of privacy laws that cover conduct by certain entities that collect certain types of information, such as information about consumers' finances or health. Various statutes address personal health data, financial information, children's information, contents of communications, drivers' license data, video viewing data, genetic data, education data, data collected by government agencies, customer proprietary network information, and information collected and used to make certain decisions about consumers. Are there gaps that need to be filled for certain kinds of entities, data, or conduct?
    - If the basic principle adopted is "Consumers own all of their personal data", then the many gaps in this list will be covered in a consumer-friendly way. We are especially concerned about inferred data. Laws controlling the collection and handling of medical records are nice, but medical information can be inferred by companies based on photos and other seemingly innocent information. It is essential that all information regarding a person's health be protected, regardless of how the information was generated. This also applies to financial, political, and other personal information. Further, as long as each state and each industry has different privacy protections, gaps will exist and be utilized in ways not envisioned by the piece-meal legislation.
- The internet is ubiquitous and global. State laws trying to regulate on-line behavior will breed confusion, uncertainty and be extremely hard for states, with their limited resources, to enforce. The United States needs one set of rules protecting all citizens' privacy. State legal frameworks can be used as guides when drafting national regulations, but will prove to be inadequate. Any federal rules need to be as least as strong as the state rules they are replacing. Short of a comprehensive law, are there other more specific laws that should be enacted?
    - The FTC should be as aggressive as possible in applying current regulations and laws. The threat of fines and other punishments will help establish the FTC's credibility in this area.

Submitted by Tom Coughlin, President, IEEE-USA on behalf of IEEE-USA

---

[i] Kosinski M., Stillwell D., Graepel T. (2013); Digital records of behavior expose personal traits; Proceedings of the National Academy of Sciences Apr 2013, 110 (15) 5802-5805; DOI: 10.1073/pnas.1218772110

[ii] Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology, 114(2), 246-257. http://dx.doi.org/10.1037/pspa0000098

[iii] Matz S., Kosinski M., Nave G., Stillwell D. (2017); Psychological targeting in digital mass persuasion; Proceedings of the National Academy of Sciences Nov 2017, 114 (48) 12714-12719; DOI: 10.1073/pnas.1710966114

[iv] https://www.wsj.com/articles/the-secret-trust-scores-companies-use-to-judge-us-all-11554523206?shareToken=ste479d62499274b62b60ebc86f18975c3&reflink=article_email_share

[v] https://ethicsstandards.org/p7000/

[vi] OMB Circular 119 (1998) including guidance on Federal agency participation in volunteer standards development at https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-119-1.pdf