October 30, 2014

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex X)
600 Pennsylvania Avenue NW
Washington, DC 20580

Re: Big Data: A Tool for Inclusion or Exclusion? Workshop - Project No. P145406

Dear Sir/Madam:

Intel is the leading manufacturer of computer, networking and communications products and has over 100,000 employees operating in 300 facilities in 50 countries. It develops semiconductor and software products for a broad range of computing applications. These platforms and technology advances are some of the most innovative and complex developments in history, and are now essential to the way we work and live. It is Intel's stated mission to create and extend computing technology to connect and enrich the lives of every person on earth. We envision the role of technology to improve education, energy distribution, government responsiveness and the delivery of health care. To support this mission, Intel works with policymakers, regulators, experts, advocates and industry to resolve policy questions related to privacy, security and intellectual property.

Intel actively pursues creative, workable ways to protect individuals' privacy. In doing so, it seeks a trusted digital environment in which data and technology can be used robustly, and in which individuals confidently can engage in commerce, conduct research, connect with friends and family, and participate in public life. In its public policy advocacy, Intel promotes dialog and collaboration between privacy policy, compliance and technical personnel so that products and services further optimal privacy outcomes.

Intel appreciates the interest that the Federal Trade Commission (FTC) has taken in big data, and its recognition of big data's positive potential and the important privacy issues it raises. In hosting the September workshop on discrimination and inclusion, the FTC highlighted the importance of addressing the social and policy issues big data raises and provided an opportunity for dialogue among policymakers, non-governmental organizations, industry and technical experts.

Intel has articulated an ambitious vision for big data and analytics. Intel believes that when used robustly, wisely, and in accordance with effective, flexible data governance, big data and

analytics promise solutions to some of the most pressing and persistent problems across society - in education, health care, economic development and climate change, to name only a few. But we can only realize this vision if we establish an environment in which individuals can trust the data environment and the way information about them is being used. In these comments, we emphasize the continued importance of existing anti-discrimination laws and fair information practices in providing necessary protections; the role of accountability; and the need for comprehensive privacy legislation to establish predictable requirements for companies and consistent, reliable protections for individuals.

I. Anti-Discrimination Laws and Unintended Consequences

We commend the FTC for highlighting the robust legal regime in place in the United States to address discrimination. We appreciate the in-depth and detailed discussion of existing US laws that protect against discriminatory practices, including the Fair Credit Reporting Act, the Equal Credit Opportunity Act, the Americans with Disabilities Act, the Age Discrimination and Employment Act, the Genetic Information Non-Discrimination Act, and employment laws under title VII of the Civil Rights Act of 1964. The FTC Act, which prohibits unfair and deceptive practices, was also cited as an applicable enforcement tool. These laws represent strong and important safeguards against discrimination that have been developed in accordance with American values and in response to public policy imperatives.

Companies using big data and analytic processing will need to take careful steps to assure that they comply with the spirit and intent of these laws, as well as the specific obligations set out in the statutes. Organizations will need to monitor carefully their use of big data and the inferences it generates to guard against the kinds of discrimination laws are intended to prevent.

For example, a bank or mortgage company is subject to the requirements and proscriptions of the Equal Credit Opportunity Act (EEOA), the law that prohibits the use of data on race and gender for purposes of determining an individual's creditworthiness. The EEOA precludes organizations from considering these characteristics in evaluating whether or not an individual qualifies for a mortgage loan. As data traditionally has been used, organizations ensure legal compliance by implementing appropriate practices and procedures to verify that such information is not considered.

Such straightforward compliance is complicated by big data analytics. While a responsible organization may take steps to remove gender and race fields from data sets, the analytics applied to predict credit-worthiness may inadvertently infer gender and race from other data (e.g., zip code, retailers frequented, product preferences) not prohibited by law. In other words, even though such factors are not directly included in the analysis, the risk of

discrimination the law is designed to prevent remains because these characteristics may be inferred indirectly and influence decision-making. Organizations will need to take care to foster compliance with existing law, which in most cases does not contemplate the nuanced way in which big data can reveal inferences, patterns and predictions about individuals. They will need to carefully consider their decisions about using certain kinds of data and algorithms that technically may fall within the bounds of law but violate its intent.

This example highlights the importance of companies' compliance with the fair information practice principle of data integrity. Companies using big data and analytics must understand the content, accuracy and currency of their data sets, and the inadvertent - as well as intended - consequences of its processing. Moreover, it stresses the importance of principles of accountability: companies must understand the risks data raises for individuals and ensure that the outcomes of big data analytics do not unintentionally fall outside the bounds of law.

II. Big Data, Analytics and the Importance of Fair Information Practices

While the example above highlights the importance of two principles of fair information practices - data integrity and accountability - Intel believes that all the fair information practices remain critical to addressing concerns about adverse effects of data use. Intel's "Rethink Privacy" initiative has called for an exploration of how fair information practice principles can be applied in a workable, practical, effective way in a rapidly changing data environment. We believe that in doing so we can make it possible both to realize the promise of big data, and to protect individuals' privacy and create trust in technology and data use.

The workshop discussion emphasized the need for transparency, the role of individual consent and the steps that must be taken when consent is not possible, the importance of data integrity and quality, and the heightened need for accountability. Participants highlighted the need for secure data collection, storage and processing, the possibilities and limits of consumer access, and considerations about purpose specification and collection limitation in an environment where data uses – and the benefits they can afford us – cannot be anticipated.

We believe that to ensure that fair information practices are effective, it will be important to examine how they can be practically applied to big data and analytics.

1. ***Openness***
   We must improve openness by enhancing transparency, and by making notice more effective. Complete and thorough disclosure of data practices can accomplish transparency by giving individuals, advocates and experts access to information about an organization's data collection practices, use of the technology, and privacy protection measures. If the public is to trust the data eco-system, it needs ready access to understandable information about how it works, and how they can navigate it safely.

2. ***Individual participation***
    a. Consent still matters, and is specifically warranted in certain instances – such as the sharing of highly sensitive data or the use of data in unexpected ways or ways that yield sensitive results. In those cases, consent should be readily available and easily exercised. But when the stakes for society are high – in cases like medical research or disaster relief – there may be an overriding interest in not making consent available. We must determine when choice is necessary and when it is not. When it isn't, internal organizational controls and accountability must be strengthened to provide the right protections.
    b. Access continues to be important to individual participation. When the processing of data affects decisions about an individual, accurate, current results depend on the ability of individuals to correct, amend or delete information. In cases where the use of data won't result in a significant decision about them, access by way of notice may be appropriate.

3. ***Collection Limitation***

    Data can be collected and stored quickly, cheaply and efficiently. Companies are motivated to gather and store vast amounts of data because it can hold the answer to unanticipated questions and be used to address problems in ways we may recognize only years from now. But the collection of data can still pose risks and decisions about data collection should be guided by rigorous risk assessment. Some data may be collected lawfully and may potentially contribute to useful analytic outcomes, but may also raise risks to individuals, or run counter to societal norms or sensibilities. Organizations should limit the gathering of data that creates a high risk of harm either to individuals or to society.

4. ***Purpose Specification***

    Big data has heightened the focus on the principle of purpose specification. Understanding what uses an organization can make of data in the context of their privacy policy is especially challenging. It is important that organizations specify the purposes for which they are collecting or using data, and limit themselves to those that are "not incompatible" with the purposes specified. More work is necessary to determine what constitutes a use that is "not incompatible," and organizations need clear criteria for making this evaluation.

5. ***Data Quality***

   Data quality - the accuracy, currency, and integrity of the data we use for processing – continues to be important. While big data analytics can yield big benefits, the predictions and insights they generate are often powerful and can affect the individual in fundamental ways. The data that supports them must be of a quality commensurate with the task, operate in accordance with the intent of the law, and yield reliable, trustworthy answers.

6. ***Use Limitation***

   Big data highlights why we need to rethink how we make decisions about the use of data, and why consent alone is no longer a logical, effective way to determine appropriate use. We need to evolve toward implementation of use limitation - a clear articulation of acceptable and prohibited uses, and assessment of risks to the individual, society, brand and reputation to determine other uses that fall between those outer limits. We need to continue to work to define the risks we must consider in doing this analysis.

7. ***Security***

   Complex data environments and vast data stores heighten the importance of security. Intel believes that organizations should implement appropriate administrative, technical and physical security. Intel also believes that the industry would benefit from industry-led security best practices that take into account the size and complexity of an organization, the nature of its activities, the risks in the use of transmission of data and the sensitivity of data.

8. ***Accountability***

   Accountability is an essential tool to promote and define organizational responsibility for privacy protection, and industry, civil society and regulators have engaged in a long term discussion to define its contours. Companies should establish policies that foster the protection of individual privacy, put in place programs and practices that further their implementation, and when asked, demonstrate that the steps they have taken are effective.

V. Comprehensive Privacy Legislation

Intel has long endorsed adoption of comprehensive, flexible, practical privacy legislation. The realities of big data and analytics emphasize the importance of adopting privacy law founded on principles of fair information practices.

Such legislation would enhance the effectiveness of existing anti-discrimination laws by broadening companies' attention to guard not only against both the possible discriminatory effects of big data analytics but also to manage data in a way that promotes the fairest, most responsible outcomes. Privacy legislation would establish predictable requirements for companies, and clear expectations for individuals. In doing so, it would create a foundation of trust that makes robust deployment of big data analytics possible.

VI. The Importance of Data Ethics

While the workshop discussion highlighted the importance of all of the fair information practices in providing protections and safeguarding against discrimination, the questions raised at the September 15 workshop highlight the need to examine questions related to big data in terms of "data ethics," and to recognize that complying with privacy laws, regulation and policy is necessary but not sufficient. In a world of big data, individuals lead data-generating and data-influenced lives. The FTC workshop highlights the reality that rote compliance with law is not sufficient, and that if we are to make innovative use of data for the most optimal, positive ends, we must take responsibility for decisions about data that foster trust and ethical outcomes. Regulation and law always trail innovation, and this area is moving quickly. The FTC workshop highlights the reality that the stakes are high for big data – both for our ability to use it for good purposes, and for the protection of individuals.

VII. Conclusion

Intel appreciates the opportunity to submit these comments to the FTC. If you have any questions about these comments, please do not hesitate to contact us. We hope to serve as a resource as the FTC pursues its work on big data, and look forward to working with you.

Respectfully submitted,

David A. Hoffman
Director of Security Policy and Global Privacy Officer
Intel Corporation