"Accountable to You"

Slide 1 - Intro

Thank organizers and moderator

I would like to show you a video that is part of Intel's effort to evolve our integration of privacy into our development processes for the changes we see coming in technology.

Slide 2 – Compute Continuum

The Compute Continuum includes devices that interface with the individual. When an individual wakes up to a pre-set alarm on their smart phone, reads the morning news on a tablet in the kitchen, obtains pollen and food allergy reports from wearable sensors in their jewelry, follows navigation guidance in what some people still call cars, but we call "computers on wheels", and then accesses their company information from both a laptop and a desktop machine during the course of their day, he or she is engaging in the Compute Continuum.

Increasingly, individuals want access to all of their data and all of their applications on all of these devices. Some of these devices will employ user interfaces which will clearly indicate to individuals how data is being collected; other technologies will collect and transfer data with little to no recognizable interface and with little or no communication to the individual about the nature of the data collection. We are embedding this Compute Continuum into peoples' lives, and now we need to Rethink how we also do this with privacy.

Slide 3 – Intel Vision

Intel supplies the microprocessors, chipsets, software and services that make this Continuum a reality, and that are used in devices across the globe. Intel's business is constantly innovating to create faster, more efficient technologies that provide better user experiences for individuals. We create innovation across the technology sector resulting in the creation of products that use Intel technology. In turn, our public policy efforts promote innovation, which can be the rising tide lifting all economies.

Slide 4 – Freedom to Learn

Intel believes that to promote innovation individuals need protected places where they can feel free to take risks, challenge the status quo and make mistakes. Privacy is critical to creating and preserving this protected space, and is therefore a fundamental element of Intel's Innovation Policy. Individuals need to have the Freedom to Learn.

The devices we use across the Compute Continuum can help provide this Freedom to Learn. These devices provide people with an unprecedented ability to communicate, create, collaborate and innovate. Given the change in how individuals will interact with this Continuum, Intel knows we

need to invest in educating our engineers on how to apply the Fair Information Practice Principles to these new technologies.

Slide 5 - Rethink

As you saw in the video, we call this "Rethinking Privacy". The effort is not to change the principles, but to provide more guidance on how to apply the existing principles in these new situations. We are not abandoning any of the concepts, and instead are focused on the need for greater emphasis and interpretation. We seek to apply global concepts, while understanding the need to respect local cultures, legal structures and histories.

While the data relating to an identifiable individual is increasing, the percentage of that data being provided directly by that individual is decreasing. At the same time the uses of that data are becoming more complex, and the potential to impact the individual is increasing dramatically.

Slide 6 – Henrietta Lacks

By way of illustration, let me use an example from a fascinating book, "The Immortal Life of Henrietta Lacks". Henrietta was a cancer patient who in 1951 had cells removed from her body without her knowledge. Remarkably, those cells have grown ever since, and have now been sold by the billions for medical research for uses from development of the polio vaccine to genome mapping. In 1951, Henrietta had no privacy rights in her cells or the information inferred from them. The application of privacy values had not yet evolved to intersect the scientific advances in cell culturing. Now that those cells have had their genome mapped, we need a separate analysis to determine whether her children and grandchildren should have any influence over how that information might be used to impact them. These immortal cells were used to create data that can live forever, and impact countless future generations of her descendants.

Slide 7 – Heather Dewey Haborg

In the same way Henrietta's cells provided information not just about Henrietta, but also about her descendants, there is considerable information out there that while it relates to us as individuals, we played little or no role in releasing it to the public. We all leave DNA around us on a daily basis. Artist Heather Dewey Hagborg has put together an exhibition of masks she actually creates from decoding the genome of DNA from pieces of gum individuals leave on the street. Similar to the gum left on the side of the street, there is an increasing amount of data about individuals readily available for complex analysis. We need to understand how our privacy principles apply to this information. Our data is out there, and it is Immortal just like Henrietta's cells.

The values that drove the creation of the fair information practice principles are similarly eternal, but we must Rethink how we use the principles to give effect to those values.

I will focus on three examples of this need for Rethinking:

1. The difference between Notice and Transparency

2. The importance of renewed focus on Security Safeguards, and
3. The critical role of Accountable and Appropriate Use

Slide 8 – Notices slide

I first want to talk about Notice.

Approximately twenty years ago companies started posting privacy policies on websites. Governments encouraged us to do so to promote the OECD principles of both Openness and Purpose Specification, and to allow for government oversight under deception standards in consumer protection law. Companies had extensive experience in lawyers reviewing advertising copy, and soon a new industry of legal drafting of privacy policies was created. Cautious corporate lawyers drafted policies to maximize flexibility for data use and minimize corporate risk.

However, when privacy policies transformed into legal contracts they stopped giving effect to the value of providing notice to the individual. For the past ten years the privacy community has experimented with short form notices, multi –layered notices, video notices, and other attempts to present the individual with information. However, a substantial body of research shows that individuals still rarely read any of these privacy policies, and when they do read them they do not understand how to apply what they read to the decisions they are asked to make.

We now enter a Compute Continuum era of technology, where many of the devices make it difficult or impossible for an individual to read something that looks like a legal contract. Further, web 2.0, data aggregation, and the increased value from data analytics mean individuals increasingly do not know who holds data relating to them. The Compute Continuum provides us with an opportunity to Rethink notice and transparency.

Regulators, academics and civil society do know who the organizations holding data are and they do read privacy policies. These are the audiences for whom we should be writing privacy policies to promote Transparency. We should move to more complete documents which fully describe the personal data collected, stored and used. While having them completely up to date for complex global organizations will be impossible, they can be held to a standard of at least regular updating. Creating these more complete descriptions provides an opportunity for responsible corporate hygiene around data. The work to develop the document will help companies understand what data they collect and maintain, why, and what mechanisms they have in place to protect it.

This would allow us to optimize for the goal of Transparency, while focusing Notice to individuals on real time context specific information that will help them make decisions, such as a message that a mobile application would like to collect location data. These context specific choices are something engineers can help design into products, and multi stakeholder processes can help define.

The Compute Continuum embeds technology into the flow of peoples' lives. We need to do the same thing with privacy. One way we can do this is by separating Notice and Transparency.

Slide 9 - Lock

The complex data environment of the Compute Continuum will put an even higher priority on the second principle I want to mention, which is security safeguards. As technology stores more data relating to individuals, we also see increased threats to exposure of the information. These threats, and the resulting increase in risk to the individual, are why we must increase our focus on the mechanisms and tools we use to secure the data.

Security, along with power-efficient performance and connectivity, comprise Intel's three computing pillars around which we concentrate our innovation efforts. In developing, manufacturing and selling commercial off- the-shelf technology around the globe, we know we play an important role in protecting personal data.

For this reason, the need for the trust of our employees, customers, civil society, regulators and individuals is a fundamental component of our global business strategy. At our heart, we are an engineering company and we pride ourselves on the engineering quality in our products. Our brand stands for great engineering, exceptional manufacturing processes, and uncompromising integrity. Individuals around the world have concerns about the security of their digital devices, and Intel stands ready to demonstrate the robustness of the development processes that support the trustworthiness of our products.

Slide 10 – IAF Logo

Mechanisms to demonstrate responsibility, like Intel's commitment to security, should focus on rethinking the concept of the third principle I want to discuss, which is Accountability. As the privacy community evolves our notion of Transparency and focuses on the need for robust Security, we need to confront the issue of the degree to which it is reasonable to expect an individual to consent to their data being processed. Unfortunately, Consent often places an unreasonable burden on individuals to understand how their data will be used, while at the same time Consent may be impossible to obtain in many contexts. We need to continue to invest in providing individuals with easier and automated methods for consenting, while also protecting privacy in those contexts where consent is not possible.

One such context, is when the personal data is provided by someone other than the individual to whom the data pertains, such as with aggregated databases intending to utilize complex analytics algorithms. The technology now is just a part of the flow of peoples' lives, and privacy must also be. It is not possible to expect individuals to continuously and explicitly consent to all collections and all uses of data. This is why it is important for us to more fully explore what is appropriate and accountable use of data. A focus on accountability and use shifts the burden from the individual back to the organization that holds the data, as it encourages responsible behavior even for situations where they can obtain consent.

Slide 11 - Values

As the privacy community Rethinks the implementation of the principles we need to focus on the need for individuals to trust their use of technology, so they can transfer data, collaborate online and innovate. The future of technology shows us an environment where we can no longer burden the individual with having to make choices about all issues concerning the processing of their data. We must increase our transparency. We must safeguard security. We must work together to define what is the appropriate use of data.

Slide 12 – "Accountable to You"

We then must develop structures which allow companies like Intel to demonstrate our commitment and show the company is "Accountable to You."