The role of the Government to promote the development and adoption of cognitive technologies

The Horse and the Zebra: Cognitive Technologies and Public Policy

Thank you so much for the kind introduction and thanks also for having me here today in beautiful Cartagena. In particular, I wanted to pay tribute to the excellent group of **speakers** that the CRC has brought together. I noticed yesterday as I met with some of you that the CRC has done an admirable job blending the internet companies with network operators such as AT+T and Telefonica as well as consumer advocates on several panels. In Washington DC where I live and work, I rarely find myself in public debates with these companies in particular and I have learned much about their perspective on public policy issues over the past few days. Thanks to the CRC for making this possible.

As mentioned, my name is Gail Slater and I am the General Counsel at the Internet Association. At the Internet Association, we represent **over 40** of the world's leading internet companies on a host of public policy issues from privacy and data security, to patents, and internet governance. Our member companies include such household names as Google, Amazon, eBay, and Facebook, as well as newer internet **sharing economy** platforms like Airbnb and Uber.

Part of our mission at the Internet Association is to study emerging technologies such as cognitive technologies so that we can **better understand** their implications in order to answer **questions** from **law makers** and **law enforcers**, **consumer advocates**, the **press**, and anyone else interested in how internet companies see these technologies interfacing with public policy.

As James from Facebook and Winston from Google explained to us yesterday companies that are investing in cognitive technologies like AI, **firmly** believe that the **economic impact** from these investments will be a net **positive** one for society.

But while Internet Association companies stand behind their cognitive technologies and the **benefits**, they also understand that public policy decision makers and consumer advocates have **legitimate questions about the potential risks associated** with these technologies and that groups like the Internet Association have an obligation to answer those questions on behalf of our industry. So with that in mind, I will try to make time for questions from you all at the end of this talk **and** we will also include in our panel discussion some questions about the role of government in promoting the development and adoption of cognitive technologies.

Before attempting to answer questions about how government **could** or **even should** regulate cognitive technologies, I wanted to first describe an **analogy** that I hope is going to be helpful. The analogy comes from the **medical field** and it has to do with how medical professionals think about diagnosing and treating patients in their care.

In the medical field, a **rare** and unexpected diagnosis is sometimes referred to as a **zebra**.

[Now, I know this may seem a strange time for a little audience participation on the subject of zebras, but bear with me. Hands up if you've seen a zebra in the past week?].

The word zebra denotes something **exceptional** and most of us are still surprised when we encounter one. I, for one, have never encountered a zebra in the wild, and I am a middle-aged mother of two who likes to think of herself as **somewhat** of a world traveler.

There's also another related saying in medical circles, **'when you hear hoof beats, think horses, not zebras."** The point here is that – unlike the zebra – the horse is a common animal throughout the world. Horses are **familiar** and most of us know what to expect from them. Again, show of hands if you have seen a **horse** in the past week or so? I know I have because I had the pleasure of visiting Old Town Cartagena and almost got trampled by one. **It was my fault, not the horses**.

The point of telling this story is that for medical professionals, **most diagnoses will be horses, and not zebras.** The chances are that the hoof beats a doctor hears as he or she is examining a patient are those of a **horse** and not a zebra, **and** the chances are that he or she will therefore know how to treat an illness based **on prior experience** using **existing** knowledge, **without** the need to consult medical journals, do **original** scientific research, or perform **experimental** surgery.

Now, you are probably listening to me thinking '**who on earth is this woman with the strange accent, and why is she giving me a lecture on zebras and horses'**!

You are right to think this. I apologize sincerely. Let me get to the point.

The point I wish to make by analogy with is this: **when it comes to cognitive technologies like AI, I think it is important to pause before regulating or legislating in these fields in new and exceptional ways. Instead, I would argue that we should take a step back and ask ourselves: are we looking at a horse, or a zebra here?** And I would argue further that if we **are indeed** looking at a **horse**, then the chances are we **already** know what to do and we can most likely apply existing laws and regulations to these technologies.

But **enough of the horse and the zebra, I promise**: The real question now becomes, what does this analogy mean from a **practical** standpoint?

Well, I think the answer to this question boils down to **three more questions** for all stakeholders involved:

- **First**, we should define the issue: what is it **exactly** that we are talking about here? What are these **emerging technologies**? After all, we can only find solutions to an issue we have clearly defined.
- **Second**, before taking action, we should do an audit of **existing laws and regulations** and ask ourselves: are they **horizontally** applicable across all sectors and verticals? Are they f**uture proof**? If so, the question then becomes, do we actually **need** new laws and regulations, or are these **existing** laws fit for the purpose? And beyond laws and regulations, are there industry best practices **already in use in neighboring spaces** that might apply to cognitive technologies?
- **Third**, to the extent that existing laws do **not** cover new technologies, we should identify what **gaps** need to be filled and ask whether we can or should craft narrowly tailored regulations to solve for this.

First off: Let's define the issue here. In deciding whether cognitive technologies are in fact **horses** or **zebras**, it is important to first define what it is they **are**, and what they **are not**. This is a simple but often overlooked point: but it's an **important** one because in order to **regulate** something, or legislate in the area, we first need to know what it is we are solving **for**.

This is particularly the case with Artificial Intelligence. Although we may not yet know the **exact** contours of AI, we did hear some consensus emerging from the panelists on yesterday's AI panel and I think we can say the following based on that discussion:

- First, we seem to have **consensus** that there is such a thing as **General AI** and that there is such a thing as **Narrow AI**. Simplifying things a bit here, we can say that **General AI** is the all knowing, **all thinking general purpose computer** that thinks and acts like a human. In

popular culture, it **could** be said that General AI is the cyborg we have all seen in movies starring, say, Arnold Schwarzenegger.

- Fortunately, as also explained yesterday, this is the stuff of science fiction even though there are still those who believe that AI may eventually be humankind's **final invention and this naturally worries them**.
- The **good news** - for me at least - is that Internet Association companies are **not** looking to build a cyborg army any time soon. Rather, they have focused their investments on solving specific problems within specific verticals. This is known as **Narrow AI**.

So going back to my horse and zebra analogy, given where most AI **investments** are being made, I would suggest that the answer to the question "**are we looking at a zebra or a horse"?** is that, at least from the Internet Association's companies standpoint, we are looking at something that **resembles a horse** much more than a zebra and this observation should inform our public policy debates.

This brings me to the **second** step in my three step process: This steps asks the questions, "if we are looking at a familiar **horse and not a zebra**, are there existing laws and regulations we can turn to in order to manage the risks associated with this technology? **Who** or **what** did we turn to in the past? And, relatedly, are there industry led best practices in place in other neighboring spaces that might help here?

I won't pretend to know what the **Colombian** response to this question might be, but I **can** speak to the U.S. experience and can focus on one important policy issue in particular – namely **consumer privacy and data security law** as enforced by the United States Federal Trade Commission or FTC, which is where I spent 10 years of my career before joining the Internet Association.

For those of you unfamiliar with the FTC, it is a **100-year old** agency that is responsible for enforcing consumer protection and antitrust laws **horizontally** across the entire U.S. economy. When it was established in 1913, the agency was handed a broad mandate by the U.S. Congress to do a number of things, including policing **"unfair or deceptive acts or practices in commerce"**.

As you can tell from these words, this is a **very broad** mandate indeed and it has provided the FTC with a lot of **flexibility** to move with the times and to adapt its activities to an ever-changing economy. In other words, as the meaning of the word "**commerce"** in the FTC's statute has changed over time since 1913, so too has the FTC's focus.

Within this same timeframe, as **new technologies** have emerged, the FTC's flexible framework has shifted to them in a relatively **seamless** way. These diverse technologies include computer hardware and software and, of course, more recently, the online internet world.

In fact, since the nineteen nineties, the FTC has become one of the world's **leading** internet privacy and data security agencies using two primary tools: the **first** is its authority to take enforcement actions against companies found to have engaged in unfair and deceptive practices with respect to privacy and data security. The **second tool** is developing **policy guidance** for industry on what the FTC considers to be good best practices in the online environment.

FTC privacy and data security enforcement actions – which result primarily in publicly available **consent decrees** or settlements– bind individual companies to l**engthy, twenty-year privacy audits**. Without **naming names,** several companies represented at this conference operate under FTC consent decrees, making the agency their **de facto regulator**. **But** I should also add that they are in good company because the FTC has taken **over 150** privacy and data security enforcement actions since it took up its role as the U.S. online cop on the beat 20 years ago.

Beyond the individual companies named in these consent decrees, these enforcement actions also serve as **precedent** to the rest of the market to follow and in this sense, these consent decrees have become the law for all companies, not just those that were investigated by the FTC.

The FTC has in more recent years used its enforcement authority to go after deceptive practices in the Internet of Things space in cases against companies like TRENDnet, which sold internet enabled baby monitors used in people's homes but did **not** adequately secure the devices. Of course, the point here is that these devices were **undreamt of in 1913** but, thanks to the FTC's flexible statute, the agency had adequate authority to investigate and take action against TrendNet as well as other IoT vendors engaged in inadequate privacy and data security practices.

Beyond these enforcement actions, the FTC also uses its statutory authority to issue **policy guidance** to industry to provide us with insights into what it considers to be good privacy and data security practices. In 2015, the FTC used this authority to convene a workshop and publish a report on privacy and data security with respect to the **Internet of Things**. The FTC report also discussed whether **new privacy** legislation is needed to cover IoT, and concluded that it was **not** because, according to the report, the **existing** FTC statutory framework was up to the task.

So going back to my medical analogy again, I would submit that these FTC enforcement actions and policy guidance suggest that the agency **itself** views the IoT as a familiar **horse** it can handle using its existing tools, and not a **zebra**.

Beyond its own immediate wheelhouse, another issue examined in the FTC IoT report was the importance of **encryption** in protecting and securing data online. In particular, the report gave favorable mention to the use of encryption to secure sensitive data in transit and at rest, in particular for data passing over consumers' **home wifi** networks. This policy guidance from the FTC deserves mention because it speaks to the role **industry** can play in creating industry-wide **technological best practices** that go even **beyond** government regulation.

Internet Association and its members agree with the FTC guidance and we believe strongly that **government support for encryption technology** will play a major role in ensuring adequate data security as new technologies enter the mainstream. **This is because online privacy and data security increasingly are safeguarded through strong encryption, and the record shows that it works: after all,** recent data breaches – both in the public and private sectors in the U.S. and also here in Colombia - have happened because firms **failed** to encrypt their customers' data**, not** because hackers broke through strong protections like encryption.

Now, we turn to step **number three** in my three steps process. This is the moment where, having argued that **existing** legal frameworks and existing technologies such as encryption **can manage and mitigate** risks associated with cognitive technologies, I cannot dismiss the possibility of a **zebra** entirely and must concede the possibility that this time is indeed different.

Some consumer privacy advocates would argue that aspects of cognitive technologies **are** different and create new challenges for society beyond the scope of existing laws. In particular, they argue that these technologies mark a big change in the **volume, velocity, and variety of data on the network (the so-called "Three Vs" of big data) and that this new era of big data, when combined with new data mining techniques, creates challenges beyond those already encountered by society**.

It's fair to say that the Three V's **are** indeed an **observable phenomenon and the numbers speak for themselves**: Machine-generated data currently accounts for only **15 per cent** of overall data. However, experts estimate that the figure will likely rise to around **50 percent** within the next decade. Alongside this **volume** increase, connected devices will deliver increased **variety** in network data, such as parameter readings, usage information, and operator behavior. Privacy advocates argue that these kinds of data might create **new** issues as they become mainstream, in particular because some of them are sensitive data that can reveal a lot about an individual consumer.

And beyond the three V's, **some** stakeholders raise real concerns about cognitive technology enabled **decision making by algorithm** and its intersection with **big data**. They are concerned that machines lack the **ethics** and **judgment** of human decision makers and worry about the impact these decisions

may have on ethnic minorities in particular in areas such as the criminal justice system, mortgage lending, and education. We heard some of these concerns raised yesterday afternoon after the panel discussion on Artificial Intelligence and we will discuss them again today.

So I do not want to dismiss entirely the possibility that we are, **indeed**, listening to the sound of hooves and hearing a **zebra**, not a horse. The question then becomes: what can we do about this **now**? I would suggest the following approach:

- **First,** I believe that we can slow down, take a deep breath, and relax. Although we are bombarded with newspaper reports talking about cyborg armies, these technologies are **not** in fact emerging at **lightning** speed (although they are emerging).
- In fact, AI has been around for several decades and has developed at a steady but relatively slow pace compared to other technologies from which it can be benchmarked, including for example **broadband internet and mobile telephony**, both of which have been around for an even shorter amount of time.
- To help illustrate this point about AI, I dug up two historic facts for you, both of them from the U.S and both of them dating back over 50 years. In **1966** the Register of Copyrights in the U.S. identified computer authorship as one of the three **"major problems"** facing the U.S. Copyright Office. In fact, the register flagged this as a **"crucial question"** for his office to answer within the next year in his annual report to Congress and yet it remains an open question to this day. We are also told that in **1960**, **President John F Kennedy** was asked to assemble a Commission to look at robots and their impact on labor. He declined to do so and life did go on without the commission.
- These 50-year old anecdotes suggests that – although we cannot **exclude** the possibility of a zebra - **knee jerk** policy reactions to AI and cognitive technologies in general are neither needed nor advisable absent evidence to the contrary. Instead, I believe we have time for thoughtful policy making and we should take it.
- **In addition to taking a step back and looking at AI in its correct historical context, I think it's also** helpful think about these technologies as **internet evolutions** and not **revolutions (with all due respect to yesterday's speaker who discussed IoT as the 4th Industrial Revolution)**.
- When you look at the internet's own timeline, I would argue that the internet **itself** has been a series of evolutions starting in the 1990's and leading up to today.
    - The **first internet evolution** created the **information graph** that changed how we produce, access, share and generate knowledge. This evolution resulted in widespread access to and **ubiquity of content online** through search engines created by the likes of Yahoo and later Google;
    - The **second evolution**, during which social media created the **social graph** that changed how we establish and foster relationships with one another. This evolution enabled power to the crowd through services such as Facebook and Twitter and the sharing economy; and
    - Next, we have the Internet of Things and AI that are creating the **physical graph,** which in turn is changing how we interact with objects and environments**.**
    - **Finally, we see today that AI and cognitive technologies are layered on top of all three evolutions and are being used by companies in all spaces.**
- The point here is that although these evolutions mark distinct and different ways through which we interact with the Internet, they all had the **internet** in common and, at least so far, these previous **evolutions** all have been **absorbed** by society using existing public policy tools such as the FTC privacy framework I described already.
- Last and **finally**, having taken a deep breath and recognized, I hope, that in may respects cognitive technologies are evolutions and not revolutions let's by all means go look for that zebra. It may only be a small one, in which case **we can fill the gap** in existing laws and regulations and move on to the next, emerging technology. **Or** it may be something larger, in

which case we may need broader legislation and regulation. But I don't believe we are there yet.

- In conclusion, I submit that when it comes to cognitive technologies we are like the doctors in my analogy hearing **a horse** and not a **zebra and we can act accordingly**. But I am eager to hear from those in the room who disagree with me and from our panel and so I invite your questions.

Thank you all for listening and I look forward to your questions and what promises to be a lively panel discussion.

ABIGAIL SLATER