***

Remarks from Chief Technology Officer, Stephanie T. Nguyen
As Prepared for Delivery
At the Department of Trade and Industry – Manila, Philippines
US-Philippines Bilateral Workshop on Consumer Protection in the Tech Sector

7 August 2023

Thank you to the Department of Trade and Industry (DTI) of the Philippine government, to the National Privacy Commission (NPC) and the US Agency for International Development (USAID) for hosting and for inviting me to give the keynote address at the US-Philippines Bilateral Workshop on Consumer Protection in the Tech Sector. It is an honor to be here with consumer protection and privacy enforcers along with representatives of Association of Southeast Asian Nations (ASEAN).

My name is Stephanie T. Nguyen, I am the Chief Technology Officer at the U.S. Federal Trade Commission. My remarks today are my own, and do not necessarily reflect the views of the Commission or any individual Commissioner.

We are here in Manila as an opportunity to share our practical experiences in the tools, techniques, and strategies in our work. We want to improve interagency cooperation beyond this event as cross-border cases and as new tech developments arise[1].

Today, I will discuss the FTC's Office of Technology, our approach, and how we apply that approach to concrete topics our team is working on alongside staff attorneys.

Further Integrating Tech Expertise in the Fabric of the FTC

Staying on the cutting edge of emerging technology to enforce the law has long been a core part of the FTC's mandate.

Earlier this year, the Commission voted[2] to establish the Office of Technology (OT), a critical resource to strengthen and support the agency's mission.[3] While the Office may be relatively new, the concept of integrating tech expertise in a regulatory agency is not. Career staff in the Bureaus have worked hard to tackle emerging harms and tech developments for over a hundred years.[4]

The direct harm to consumers often is a symptom of some underlying structure that facilitates that harm. The Office of Technology understands how the basic layers and building blocks of technology – from the architecture to the design – are vehicles and artifacts of harm.

OT seeks to identify and treat that underlying structure. Otherwise, we are just walking into a house that is crumbling at the foundations and only focusing on painting the walls. The rot is still there.

--

Some Challenges We Face Today

In the 1890's fourteen-year old Abigail Roberson arranged to have professional studio photos taken of herself.[7] A few months later, she stumbled on a poster advertisement for Franklin Mills' flour with her face – one of the thousands of the same ads displayed in public grocery stores. This story of unauthorized circulation of one's personal data, information, or photos is just one of many. And on top of that, women's faces and bodies, more often than men, were the "subject of surreptitious photographs" used for commercial efforts[1].

Fast forward to just a few weeks ago, the Office of Technology had our first full team gathering in Washington, DC. My colleagues outlined the number of times our personal information was picked up. On Monday, the team got lunch at a local restaurant, which required us all to scan a QR code to place an order to put ourselves on a waitlist. On Tuesday, we went to a work gathering at a venue, where our IDs were scanned into an app, gathering our names, birthdays, address, credit card numbers, and gender. The team noted some trends:

1. First, it is increasingly difficult to exist in society without being tracked in some way. In living, working, and just being – our information is collected at many touchpoints in our day to day.
2. Next, more information may be collected and shared than one would think at one of those daily mundane touchpoints. For instance, a photo containing geolocation metadata could potentially be scraped by a website for which you upload that photo to post about your homemade fried lumpia.

Recall the era of using folded paper maps and printing out directions to a new place. People slowly graduated to a talking GPS device attached to a suction cup on our car windshields. Fast forward 20 years, millions of people now have GPS equipped smart phones in their pockets, broadcasting our highly precise location to anyone they want – and unfortunately to a bunch of people they don't want.

These consumer harms are not just one-offs, they are happening at scale and can be exacerbated by dominant gatekeepers. Our team is working with the Bureau of Competition to ensure open and fair competition, including at key inflection points as tech develops.[10]

Our world has significantly changed since the 1890s, but some things have remained the same. Technology continues to expand and increase the speed of information sharing in ways that are known or unknown to consumers at scale. Companies will continue to find ways to advertise and track our behaviors and interests to increase their bottom line. And increasingly, the lines between what is a "tech company" and what is not is blurred. Given the ongoing rise of the digital economy, it is critical that we build capacity to parallel these shifts.

Our Approach

Before we get into our work – I'll discuss our approach: envisioning an outcome, evaluating historical tech shifts and checking outdated assumptions.

[1] Sarah Igo, The Known Citizen: A History of Privacy In Modern America.

--

[Envisioning outcomes: innovation, dynamism, consumer choice & job mobility]

We received over 700 applications from talented individuals since launching the Office. We've had the opportunity to interview excellent technologists across the United States. Beyond sharing their expertise, some share their career goals to drive meaningful change at a law enforcement agency.

What has been inspiring to me is that candidates express optimism over defeat – flagging the chance to drive positive outcomes for consumers and for the market. We need enforcement for small businesses to be able to innovate and compete in a level playing field.

For instance, a cancer patient should be able to travel to treatment facilities without having their location shared to third-party advertisers.[11] Prospective tenants should not be denied housing due to inaccurate background reporting.[12] Employers should be able to compete for the best skilled workers.[13] And a new startup should be able to enter the market, grow, and thrive without risking being cut out by dominant gatekeepers.

Bringing this many incredibly talented technologists into our agency creates an opportunity to strengthen the ways that we approach our enforcement and regulatory mission. At the Office of Technology, we are looking to seize this opportunity to create key shifts in the way that the agency approaches technology. But the foundation starts with people and with understanding the importance of how history plays into our current moment.

--

[Examining the history of platform shifts]

Once we have a goal in mind for the future state, we must look back and study historical platform shifts that have impacted consumer behavior and business models.

In the 1990s and early 2000's, brick-and-mortar businesses transitioned to the internet. New technology changed consumer online shopping habits, including price comparisons to purchases and returns. E-commerce platforms collect troves of information about us and can expose us to risks. This includes the risk of sharing sensitive data that could impact one's personal privacy or high stakes decision-making including housing access and job opportunities. People no longer line up outside of gaming shops to get the latest gaming console. Companies can create highly curated content for personalization and generate recommendations to continue consuming that content.

And now today – with generative AI, we are shifting from information curation to creation – where generative models can take a large dataset of existing content, learn patterns and relationships and then generate more content through images, text, and video.

--

[*Check outdated assumptions*].

Beyond historical shifts, it's important to check outdated assumptions about how tech markets work to meet modern challenges. Some may believe that companies can self-regulate and markets will correct themselves.[14] As Chair Khan stated in an op-ed on AI[15], when government action required AT&T to open up its patent vault it "unleashed decades of innovation and spurred the expansion of countless young firms."[16]

We must also dismantle outdated paradigms about regulation. This is why agencies like the FTC exist. We have a responsibility to enforce against unfair or deceptive acts or practices or unfair methods of competition - especially as these practices evolve with new tech advances.[17] Enforcers should enforce the law and companies should take responsibility to abide by those laws. I'll now explain a few ways we should check outdated assumptions.

> *Paradigm shift #1:* The burden should not be borne by consumers to navigate complex terms of service to use a product or service. As research has shown for years, privacy policies and forms of notice and consent are "practically and inherently insufficient," especially if they constantly change and are riddled with complex user data flows.[18] And, there's no reasonable alternative. If you don't accept the terms, there's no choice – just the illusion of choice.
>
> *Paradigm shift #2:* Practitioners, researchers, civil society, and journalists are a critical source of accountability and transparency in our society. They should not be expected to provide free services to improve corporate products. And everyday consumers shouldn't be treated like guinea pigs for poorly conceived products.
>
> *Paradigm shift #3:* The responsibility doesn't end with the engineers and designers who built the product. They're one layer in a broader system designed by executives to achieve their bottom line. In fact, a recent FTC complaint[19] alleged that a UX team got no traction with leadership and executives on their recommendation to make certain feature changes that would establish more privacy protecting configurations. Even a well-intentioned design team's decisions can be twisted or subverted by the motivations of their executives and underlying business models.

--

Our Work: Investigating the Layers of Technology and Tech Practices

We've contextualized how these technologies have shifted over time and have checked outdated assumptions.

Looking at both the layers and tech practices allows a better understanding of the product – and allows the FTC to anticipate likelihood rather than only react to harms.

I'll walk through two key concepts – tech layers and practices.

--

[1 - *Layers*] Our team of senior technology experts seeks to understand not only emerging technologies as they play out in the marketplace but also how harms develop and manifest through various layers of a product. So we must examine all layers of the technology– including the infrastructure, models, data, and the user-facing design of a product.

The layers we consider move from the foundational tech at the bottom of the tech stack, starting with the development processes and infrastructure used to create the system, and the underlying cloud hosting for most modern technology. From there, we think about the details that are most critical at the application layer – this includes models and algorithms that products use to make decisions, as well as the collection and management of user data. Finally, we look at the user facing elements of the product, the user experience and design.

[Infrastructure] Infrastructure and security engineers can help identify negligent security or infrastructure practices. For example, an infrastructure engineer may ask about how encryption keys are generated or stored. In a prior FTC Open Commission Meeting, OT presented on three key security principles, drawing from recent order provisions from data security and privacy cases.[20] To address the underlying causes of risk in complex systems, we highlight three key areas. First, offering multi-factor authentication for consumers and requiring it for employees. Second, requiring that connections within a company's systems be both encrypted and authenticated. And third, requiring companies to develop a data retention schedule, publish it, and then stick to it. OT's work, in coordination with our Division of Privacy and Identity Protection highlights these principles reflects the Commission's focus to keep pace.

[***As a subset of infrastructure, cloud computing*]** The FTC launched a Request for Information (RFI)[21] on cloud computing providers. These companies create a network of servers on the internet to digitally store, manage, and process data (as opposed to physically managing these resources). Cloud computing is a critical part of sectors including healthcare, banking and finance, entertainment, and transportation.[22] In addition, emerging technologies such as generative AI products and services (like chatbots) are computationally intensive and are reliant on such providers. In our RFI, we highlight a wide array of issues. We cover the potential for single points of failure. If large swaths of the economy are reliant on a handful of cloud computing providers for the infrastructure that powers AI, houses data, hosts websites - any issues with those cloud offerings have widespread and significant implications. Next, we cover security in cloud computing which raises the question of how responsibility for securing customers' personal information should be shared between cloud providers and their users. And finally, we cover market power and business practices affecting competition in cloud computing. The FTC is diligently working on analyzing the submitted comments to determine potential next steps.

[Models] Moving to models, technologists can analyze machine learning models and understand how these systems learn and make decisions in ways that may impact people's health & access to opportunities. In the FTC's complaint against Everalbum, a photo app developer allegedly deceived consumers about the use of its facial recognition technology without affirmative express consent – combining millions of facial images obtained from publicly available datasets to enhance its face recognition technology. The order required the deletion of data, models and the algorithms that the company developed.[23] In addition, through an AI report on "Combatting Online Harms Through Innovation,"[24] staff previously highlighted that unrepresentative datasets used to power AI models can result in bias or discriminatory outcomes.[25] Thinking ahead, the FTC has outlined how models are being developed in generative AI. In a post on AI and Competition,[26] we described how models are trained on large amounts of data, which can be used to make decisions and predictions. Competing for the best talent in machine learning, natural language processing and computer vision is also critical to develop and maintain models that are quickly evolving.

[Data] Technologists can help unveil how data might be collected and used across the product lifecycle which could lead to exploitative data sharing practices.[27] The Bureau of Consumer Protection announced several cases involving consumers' sensitive health data including BetterHelp[28], GoodRx[29], Premom[30], and Vitagene[31]. These cases outline that unauthorized disclosure of consumers' health information which can range from fertility to prescriptions to mental health may violate the law[32]￼ We also help translate how complex data flows may work. The ability to understand how data is collected, used, shared, and tracked is critical for understanding industry conditions, competitive dynamics and business advantages. We wrote a post on a type of data tracking called pixels – code embedded into a website or app which can send all sorts of personal data including purchases and online behaviors[33]￼

[Front End Design] Designs are directly tied to a business's incentives and motivations. Every product or service is built with an end goal or purpose in mind – which impacts the screen design, user flow, and information architecture. By examining the front end and user interface of worker surveillance technologies for example, we can help unpack how certain features can lead to harms. For instance, certain employee monitoring software may lack any indication that they may be collecting data when employees may be off duty – collecting or sharing their location data or sensitive health data which may lead to adverse outcomes. Relevant to casework, in the Epic Games / Fortnite case[34], the voice communications settings were set to on-by-default and were difficult to find and turn off if users wanted to opt out. These default settings, the FTC alleged, "along with Epic's role in matching children and teens with strangers to play Fortnite together, harmed children and teens."[35]

--

[2- *Tech Practices*] Now that we've covered some core layers of technology, we will move to tech practices. Some companies may launch beta versions of experimental products that could produce errors or may try to evade liability by launching a beta version and having disclaimers. Just because companies disclose that something is experimental or untested does not mean that they are immune from the law, especially if there is substantial harm or injury to consumers. Whether the product is launched to ten people or ten million people – we can't only look at harms *after* they've occurred. In fact, it is a longstanding principle of FTC rules, enforcement, and guidance that companies should be taking proactive steps to prevent foreseeable harms:

- The agency has brought legal actions[36] against organizations that have misled consumers by failing to maintain security practices[37] to protect sensitive consumer information.
- Second, the Red Flags Rule[38] requires that businesses and organizations implement procedures to prevent and mitigate identity theft *before* it happens.
- Third, our Safeguards Rule[39] establishes standards for safeguarding and protecting the security of financial institutions' consumer information. The rule was amended in 2021 and highlights nine elements that a company's information security program[40] must include – ranging from qualified individuals to supervise to implementing multi-factor authentication[41] for anyone accessing customer information on your system.

--

A Sustainable Strategy Moving Forward

For our Office of Technology to support the agency to continue delivering in its investigatory and enforcement work, we need to first be able to build a strong team.

A sustainable strategy is necessary to adapt to such shifts in technology. This means being rooted in the benefits of regulation, checking outdated assumptions and examining the history of platform shifts. It also means applying our knowledge of how tech works in practice. The Office of Technology is tackling pressing issues as it applies to layers of technology outlined above – emphasizing prevention over detection and thinking of ways to intervene more upstream than downstream.

Fifteen years ago, the term "cloud" may have sounded like a marketing buzzword, my colleague shared.[42] "Now, many companies no longer own or operate any of their own physical servers, and instead they've migrated to cloud servers […] and sometimes infrastructure that's even further abstracted from hardware."

Tech evolves daily. Just as the agency has cultivated tech savvy lawyers – we are building resilient, law savvy technologists who are working directly on cases and enforcement to use their abilities to understand tech systems and structures and get at the root cause of harm.

Thank you.

***

Thank you to my FTC colleagues for your contributions to these remarks and to the indefatigable OT crew for which this Office would otherwise not exist. Jessica Colnago, Simon Fondrie-Teitler, Alex Gaynor, Crystal Grant, Amritha Jayanti, Nick Jones, David Koh, Sam Levine, Josephine Liu, Erik Martin, Kevin Moriarty, Ben Swartz, Mike Tigas, Maddy Varner, Holly Vedova, Ben Wiseman