Remarks of FCC Enforcement Bureau Chief Loyaan A. Egal
Media Institute – Communications Forum Luncheon Series

As Prepared for Delivery – Thursday, November 9, 2023
St. Regis Hotel, Washington, DC

Thank you, Rick, for that kind introduction, and thank you everyone for attending today. Also, thank you to Chairman Wiley and everyone else at the Media Institute for the invitation to join you today. I had the distinct pleasure of attending the Media Institute's Free Speech America Gala last month and truly enjoyed being able to hear Bob Woodward, Michael Powell, Curtis LeGeyt, and Donald Graham speak at that event.

As the last speaker in this year's luncheon series, I took a look at the remarks of the distinguished speakers who preceded me in 2023. Talk about no pressure. Blair Levin began the year by identifying things he believed were not being talked about or were being talked about in a weird way and was able to weave in topics involving TikTok, broadband maps, spectrum, and ACP in a very interesting way. Vint Cerf, Chief Internet Evangelist for Google and the penultimate speaker in this year's series, spoke about the history of the Internet and the technologies that will be needed to communicate in deep space in the next decade. Mr. Cerf is also known as the "Father of Internet." I, on the other hand, am simply the proud father of two wonderful children.

The theme that cuts across these remarks is the critical nature of the communications sector. While I won't be able to describe what I find being talked about in a weird way, or talk about what Star Trek-type technologies are on the horizon to assist us with exploring deep space, I can provide you with insight into what we at the FCC's Enforcement Bureau do to ensure a robust and trusted communications sector. We want innovations to flourish and protect consumers' privacy and sensitive data and the nation's security.

THE ENFORCEMENT BUREAU AND ITS HISTORY

But first, let me tell you a little bit about the Enforcement Bureau, which is home to an amazing group of talented public servants, and which I have been proud to lead for a little over 21 months.

EB dedicates its resources to investigations and enforcement actions involving FCC-regulated services, equipment, and programs that significantly impact:

- Consumer Protection and Privacy;
- Data Security, Cybersecurity, and Supply Chain Integrity;
- National Security, Public Safety, Emergency Services, and Harmful Interference;
- Fraud Targeting Critical FCC-Funded and -Administered Programs; and
- Fair Competition and Equal Opportunities.

I like to point out that even though it was established last century, the Enforcement Bureau is

only 24-years old having been created in 1999 under the leadership of Chairman William Kennard. Therefore, next year we will be celebrating our Silver Jubilee to commemorate our 25 years of existence.

For context, even though the Securities and Exchange Commission and FCC both came into existence in 1934, the SEC has had a Division of Enforcement since 1972.

The inaugural front office leadership of the Enforcement Bureau consisted of David Solomon (Chief); Brad Berry and Jane Mago (Deputy Bureau Chiefs); Richard Welch (Associate Bureau Chief); and Arlan van Doorn, John Winston, and Suzanne Tetreault (Assistant Bureau Chiefs). I like to refer to them as the OGs of EB.

As the sixth chief of the Enforcement Bureau, I follow in the footsteps of the aforementioned David Solomon; Kris Montieth; Michele Ellison (the current general counsel of the FCC); Travis LeBlanc; and Rosemary Harold.

One other piece of trivia I like to share about the FCC and the Enforcement Bureau is that we are statutorily authorized, along with the Department of Justice, to enforce the Wire Fraud Statute (18 U.S.C. § 1343). I remember when I first found out about this and had to tell myself: "You've got to be kidding! You can't tell a former federal prosecutor he can charge wire fraud without having to worry about things like venue." Lo and behold, it turns out that when the Communications Act was amended in 1952, it resulted in also amending Title 18 of the United States Code to introduce Section 1343.

Fast forward 71 years later when last week you may have seen in the news that my old office, the U.S. Attorney's Office for the Southern District of New York, was able to secure a conviction of Sam Bankman-Fried for, among other things, conspiracy to commit wire fraud and wire fraud for a multibillion-dollar scheme involving the FTX cryptocurrency exchange. This highlights for me the foundational importance communications services and networks play in our society, and the importance that must be placed on ensuring their availability and integrity while mitigating efforts to compromise them, steal valuable and sensitive data, or use them to defraud people.

THE FCC'S UNIQUE PERCH

When I was asked to come back to the Commission to lead the Enforcement Bureau, I joked that I was going to go from working on national security-related matters every day inside a sensitive compartmented information facility (SCIF) to now holding my breath during the Super Bowl halftime show and the Golden Globes. Turns out the joke wasn't far off. The Will Smith/Chris Rock Oscars incident took place less than two months into the job. If you're curious, there were 66 complaints filed regarding that incident.

But when you think about everything the FCC regulates, which stretches from under the ocean with fiber optic submarine cables that physically connect the United States to the rest of the world—and through which approximately 99% of global voice and data services traverse—to outer space when it comes to satellites, and a whole lot of things in between, the breadth and scope of the enforcement possibilities are unlike any other. As a sector-specific rulemaking

agency with enforcement authorities, the FCC is *sui generis* vis-à-vis its sister regulatory agencies. I'll try to keep the Latin/French expressions to a minimum.

A few examples to help illustrate this scope and uniqueness. The FCC administers multibillion-dollar programs (the Universal Service Fund and the Affordable Connectivity Program) aimed at assisting low income and rural communities with having access to vital information and communications services. But agencies that oversee large federal programs such as the Social Security Administration (SSA) or Health & Human Services (HHS) do not have a regulatory enforcement arm and have to rely almost exclusively on their Office of Inspector General and the Department of Justice to address fraud targeting their programs. Meanwhile, the FCC enforces the statutory and regulatory requirements associated with its programs, and the Enforcement Bureau has regularly conducted parallel investigations with the Department of Justice, brought enforcement actions, and entered into global settlements addressing fraud. Just this year, the FCC along with DOJ agreed to a more than $40 million global settlement to resolve the Enforcement Bureau's and DOJ's parallel investigations into violations of the Commission's competitive bidding rules and the False Claims Act involving the USF Rural Health Care Program.

The FCC is the only agency with consumer protection responsibilities that also directly regulates entities that qualify as critical infrastructure, which has been defined by Presidential Policy Directive-21 to include the communications sector. Because of the interconnected and interoperable nature of terrestrial, satellite, wireless, and submarine cable-facilitated networks, the FCC is the only regulatory agency that has an established process, the Team Telecom Committee process, to assess national security and law enforcement risks as they pertain to foreign investment and ownership in the domestic communications infrastructure. Last year, we announced a consent decree in which a company named Truphone admitted that it failed to disclose accurate foreign ownership and transferred control of FCC authorizations and licenses without Commission approval, which circumvented the Team Telecom foreign investment and ownership vetting process. As part of the settlement, the company paid a $600,000 fine and was required to divest Russian ownership interests and ensure that all foreign investment complied with the Treasury Department's Sanctions List.

This summer we issued the largest ever FCC fine, almost $300 million, against a group of U.S. and transnational companies that were responsible for billions of illegal robocalls that were hawking auto warranties. Our unique enforcement authorities to direct the voice communications sector to take steps to effectively mitigate the auto warranty calls we identified in our investigation resulted in a 99 percent drop in those types of calls.

Just last month, the Enforcement Bureau entered into a first-of-its-kind consent decree with DISH to settle an investigation into the company's failure to comply with its satellite deorbiting plan. That settlement included an admission of liability and a $150,000 penalty. As the world's first-ever fine involving space debris, it made clear that the U.S. government is serious about enforcing the rules governing satellite orbital operations.

ENFORCEMENT PRINCIPLES

As you can imagine, my prosecutorial and national security background informs a lot as to how I approach the enforcement challenges the FCC faces. Listening to Bob Woodward a few weeks ago spell out the principles of investigative journalism he believes help rebut distrust and contempt of the media resonated with me. We apply the ABCD Principles of enforcement to help ensure that public trust in our approach is not misplaced.

Those principles are:

- Accountability;
- Balance;
- Compliance; and
- Deterrence

We need to ensure that those who violate the Communications Act and FCC regulations are held **Accountable**. Our rules are not suggestions; they're obligations. It's our job to hold wrongdoers accountable. Companies should not consider breaking the law as simply the cost of doing business. That means, when appropriate, requiring admissions of liability as part of our settlements.

In exercising our enforcement authorities and prosecutorial discretion, we strive to make sure that we are striking the right **Balance**. That means taking a holistic approach and considering all relevant factors in making an enforcement decision.

Through our enforcement actions, we seek **Compliance** with statutory and regulatory requirements, which for purposes of our settlements typically includes a compliance plan to address the specific concerns that gave rise to the issue we are addressing.

Finally, when we take an enforcement action, we do so with the two specific goals of achieving specific and general **Deterrence**. Specific deterrence with the party against whom we are taking action to ensure that the violative conduct is addressed going forward. General deterrence for those considering engaging in similar conduct.

PRIVACY/DATA PROTECTION/CYBERSECURITY

I would like to now focus the remainder of my remarks on the work of the Enforcement Bureau and its role in spearheading the Privacy and Data Protection Task Force. First, a little bit of table setting. According to the Pew Research Center, 97 percent of adults in the United States have a mobile phone and 85 percent of those adults have a smartphone. With that level of market penetration, few things in our society are as ubiquitous as cellphones.

As Chairwoman Rosenworcel stated when she established the Task Force:

> We live in an era of always-on connectivity. Connection is no longer just convenient. It fuels every aspect of modern civic and commercial life. To address the security

challenges of this reality head-on, we must protect consumers' information and ensure data security.

The amount of sensitive data we generate using these instruments—who we speak with, where we are located, what we read, and where we bank or what we purchase, to name a few—and then entrust with the companies that provide us these connectivity services is unprecedented in our history. Collectively, this is referred to as "Pattern-of-Life" information, because it creates a detailed profile of who we are, where we live and work, and who is a part of our social and familial networks.

When nation-state threat actors gain access to these bulk datasets telecommunications carriers collect and store, it can enable computer hackers and intelligence officers to better target those in the government, military, and other sensitive roles, which creates a national security risk.

I understand from a press report that at the NTCA Telecom Executive Policy Summit earlier this week, DHS Cybersecurity and Infrastructure Security Agency (CISA) Executive Director Brandon Wales stated that we are currently in an acute period of heightened threat, and that sophisticated cybersecurity threats from cybercriminals and foreign adversaries are "prepositioning" for a future attack on the United States. Even more ominously, he stated that it is the worst that he's seen in the 20 years that he has worked on homeland and national security issues, and that telecom network operators must play a pivotal role because the government by itself can't stop everyone that wants to do harm to the United States.

For our part, and consistent with Mr. Wales's clarion call, we have more than doubled the number of people handling these cases and hired individuals with privacy and data protection experience. Jolina Cuaresma, who most recently served at Common Sense Media as Head of Law & Tech Policy has joined the Enforcement Bureau as a Senior Policy Counsel. By early next year, the Enforcement Bureau's front office will have four senior officials with significant DOJ and interagency experience on national security, foreign investment, data protection and cybersecurity, and consumer and civil litigation matters.

Now, how do we approach our enforcement investigations in this space? Privacy, Data Protection, and Cybersecurity are three distinct disciplines that many times have significant overlap. Privacy is fundamental to our liberty and its sanctity must be protected. That means looking at how FCC-regulated entities are treating the data they have been entrusted with as part of the customer/service provider relationship. Data Protection goes to how service providers protect the sensitive information with which they have been entrusted. Cybersecurity focuses on how those companies protect the networks in which the sensitive data is housed. Our investigations can touch on one or all of these disciplines.

From a Task Force perspective, the Task Force coordinates across the agency on the rulemaking, enforcement, and public awareness needs in the privacy and data protection sectors, including data breaches (such as those involving entities providing FCC-regulated services) and vulnerabilities involving third-party vendors that service Commission-regulated communications providers.

- **SIM Swap/Port-Out Fraud Rulemaking**: The Task Force recently announced new proposed rules to protect consumers against scams involving SIM Card Swapping and Port-Out Fraud – these schemes have become more and more commonplace and law enforcement agencies are keenly aware of these schemes being scaled up throughout the country. The Chairwoman shared final rules with her colleagues and they are under consideration as we speak.

- **Q Link and Hello Mobile**: The Commission proposed a $20 million fine against Q Link Mobile and Hello Mobile for failing to protect consumer privacy. The proposed fine made clear the company's apparent failure to protect the privacy and security of subscribers' personal data. The companies apparently failed to authenticate customers' identity before providing online access to Customer Proprietary Network Information (CPNI).

Our teams handling privacy/data protection and scam calls/text enforcement matters are working together given that many times information harvested from data breaches can be used by bad actors to defraud people through carefully tailored targeting using their compromised sensitive information.

CONCLUSION

As the previous speakers made clear, the communications sector is vital to who we are and how we live our lives. As part of the nation's critical infrastructure, FCC-regulated companies provide essential services that underpin our society. The pandemic served to highlight just how integral these companies are—from making telehealth visits possible to bringing educators into our living rooms. And our job in the Enforcement Bureau is to ensure that the public's trust in these companies isn't misplaced.

The depth and breadth of the impact of these technologies and services are vast.

And when I think about our work in the Enforcement Bureau—and our collective effort to fulfill the FCC's mission to protect consumers, protect the national defense, and ensure that the public's trust in our communications networks isn't misplaced—I think back to just a couple of days last December before Christmas.

On December 20th, the D.C. Circuit affirmed the FCC's ability to revoke the section 214 authorization of the U.S. subsidiary of China Telecom, a Chinese State-Owned Enterprise telecommunications company, highlighting the Commission's authority under the Communications Act to regulate the nation's communications infrastructure in furtherance of "national defense."

I recall working on this case at DOJ several years prior and helping lead the interagency effort to submit the national security recommendation to the Commission.

A day after this landmark decision, on December 21st, at the Commission's open meeting, the FCC unanimously issued the "Notice of Apparent Liability" following the Enforcement Bureau's investigation for the matter I previously mentioned involving auto warranties.

When I stepped back to think about these two events, they demonstrate the vigilance required to keep our communications networks safe and enhance the public's trust in them. And my job is to ensure that the Enforcement Bureau will remain ready to meet this moment. And we will be.

Thank you.