COMMISSIONER SIMINGTON ADDRESSES SILICON FLATIRONS 2024 FLAGSHIP CONFERENCE: GLOBAL FRACTURES IN TECHNOLOGY POLICY
FEBRUARY 5, 2024

Good morning everyone. Thank you for being here today for this early session. I'm excited to talk to you about what I think will be an unsettling future reality: the accelerating move from a single Internet and technology market toward one fragmented along national borders due to concerns about digital sovereignty.

There was a lot of heady idealism in the early days of the Internet. The internet was a universal, open network where people from around the world could exchange services and ideas basically without restriction. There were no borders online. If you put up a web site in the United States, someone on any other continent could access it just as well, if a bit more slowly, than someone else in the US. Across the world, people were using the same devices, running the same software, usually with no more modification than a local translation of the user interface. "Information wants to be free" was a common slogan. Free as in speech, not as in beer (though there was a certain amount of the latter as well.)

There was universal condemnation of the places where information was not free. China's Great Firewall—their massive internet censorship apparatus closely monitoring and restricting all traffic in, out, and within China—was seen as something obscene, a contemptible practice out of a dystopian novel, a crime against our open future and something that should be universally resisted. But today, China's behavior is not as much of an aberration as it once was. Restriction of access to foreign websites, or restrictions by the sites themselves of content in accordance with the user's location, is routine, practiced or required by governments on practically every continent and of every kind: democracy, monarchy, and one-party. Even when allowed, foreign online services are often viewed with growing suspicion. Governments avoid devices from certain countries, and sometimes even prohibit their citizens from buying them. The idealism of the early Internet might survive in some ways, but it now has to accommodate concerns about backdoors, espionage, foreign propaganda ("election interference"), and cultural influence.

This was probably inevitable, because governments were going to both see political advantage and receive constituent demands for the same kinds of restrictions that had existed on earlier communications, media, and industrial technologies. We are now in a strangely liminal space. Eternal September was over 30 years ago; I was 14 when it happened (and I note that this was about one year after the NSF handed internet governance over to the Commerce Department, another watershed.) Those of us over 35 or so experienced a largely free Internet, those of us over 55 likely experienced an Internet still rooted in the ARPANet, but those of us younger than this will have few such memories, perhaps experiencing this era only through the Space Jam website or mid-90s "how to get online" videos posted to Youtube—a platform that is now itself old enough to be in college.

One of the most important fractures is the growing divergence in the kinds of content and viewpoints that countries are willing to allow online. Major fissures are opening even between the US and EU, to say nothing of other countries that don't care much for free speech at all. Even

the United States, with the strongest free speech regime in the world, has increasingly taken to alarm about foreign influence operations online, inviting federal government efforts of questionable constitutionality. Individual European countries and the European Union as a whole have adopted policies requiring that technology companies censor content promoting various ideologies. Googling for the same content in the United States, Germany, and China, can return vastly different results, in large part due to the different content regulations in force in those countries. And, of course, in Canada some social media platforms have completely exited the practice of linking news stories at all.

If the EU wants to ban what it perceives as hate speech, but a US social media network adopts a strong free speech stance, what is Europe to do? If the company has European offices, it could assert jurisdiction on them, but suppose the company closes its European offices but continues to allow European users to access the site. Does merely allowing users to access a site give the country those users are located in jurisdiction over the website? If yes, then it's easy to see how the internet will quickly fragment into national internets with selective, regulated interconnection with other countries. If no, then what will Europe do? Punish citizens for accessing the site? Develop a Great Firewall like China to prevent citizens from viewing offensive content? There are no great options, but it is hard to see how a single, open internet can survive these pressures.

Speech and content aside, another potential source of divergence is the national nature of competition—what we Americans call "antitrust". Because of the international reach of the Internet, mergers and other arrangements between American media and technology companies are now matters of importance to governments around the world. Likewise, technology companies located overseas that have large numbers of customers in the United States—say TikTok, TP-Link, Lenovo, Siemens, Erikson, Sony, and Nintendo, just to name a few—could feasibly enter into arrangements that raise antitrust concerns in the US government. The US and EU have already had minor spats about competition law as it pertains to companies like Google and Microsoft, and it is only a matter of time before more major conflicts arise between competition regulators in different countries, and one result could be the fragmentation of internet and technology markets along national borders.

Of further concern is the potential for foreign technology devices and services to be vehicles for espionage and sabotage. Hiding backdoors in software is trivial, and even when discovered, it can be impossible to distinguish a backdoor from an inadvertent coding mistake or sloppy design. We really cannot be sure that any non-trivial device from China, be it a network router or a laptop or a cellphone, can be trusted to not contain backdoors that would allow the Chinese government to exfiltrate data, take control of the device, or render it inoperative. In fairness, they probably feel similarly about American products. And the same concerns apply to online services. My colleague, Commissioner Brendan Carr, has been sounding the alarm about TikTok gathering the data and private communications of millions of Americans, and I am in total agreement with him. But those same concerns must ultimately extend to any services that store data about Americans in adversary countries, or countries and companies that could easily come under the influence of those adversaries.

Even the most seemingly benign use of foreign technology can become a security threat. GPS, developed and controlled by the US military, was once the only satellite-based global positioning and precision timing system in the world. But now it faces competition from foreign alternatives like the EU's Galileo, Russia's Glonass, and China's BeiDou. Supporting those systems is sometimes a requirement for device manufacturers wishing to sell in those countries. So between the economic incentives (such as economies of scale) for manufacturers to have a single model for all markets, and the fact that these positioning systems sometimes offer higher precision than the American GPS system at the moment, it appears that many American businesses and consumers are knowingly or unknowingly relying on these foreign systems in their operations. At first it might seem that there is not much risk. After all, these are receive-only systems that do not involve any transmission from receiving devices back to the satellites. (A quick note, the Chinese system does have a higher-accuracy two-way mode, but let's put that aside) But if these timing and positioning systems are being used to guide precision industrial and commercial processes in the US, then our adversaries could potentially cause widespread disruption to by shutting down access within the US or, even worse, intentionally returning incorrect data to American receivers of their signals.

I don't want to be misunderstood. The end of the universal, open Internet and technology market that I fear is coming is not good for the United States. We have the best technology companies in the world, and we benefit immensely from their access to world markets. And people in other countries benefit immensely from access to cutting-edge technologies developed in the United States. The same goes for American access to technologies developed abroad. As moves toward technological sovereignty progress, the United States needs to do everything in its power to develop workable arrangements with our allies, and with the great majority of countries that have no quarrel with us, nor us with them. These arrangements need to balance sovereign interests with the mutual benefits of open markets.

With these principles in mind, I'd like to turn now to some examples of what the FCC has been doing with regards to digital sovereignty, as well as suggestions for further FCC action.

In 2019, Congress passed the Secure and Trusted Communications Networks Act. It directed the FCC to ban any companies receiving FCC subsidies from using certain Chinese networking equipment in their networks, on the theory that such equipment could be a trojan horse, as I explained earlier. Then in 2021, Congress passed the Secure Equipment Act, which directed us to ban those certain Chinese companies from having any new devices approved for sale in the United States, as well as to explore the possibility of prohibiting the sale of their previously approved products. These are great laws, and our implementation of them has been robust so far.

But ultimately, these are only band-aids for a deeper problem. Faced with a choice on the market, businesses and consumers are often making the decision to buy untrustworthy equipment from China companies instead of Western-made alternatives. And trusting Chinese equipment is not the only seemingly bad security decision they are making. Over and over again, they buy products from companies that fail to take security seriously, that are careless in their software development practices, that fail to patch known vulnerabilities in a timely manner, and that don't even take the most basic precautions to prevent unauthorized access and control of their devices.

So while further bans of potentially hostile equipment are necessary, they won't be enough. We need to figure out how to get consumers to choose secure products over insecure ones. I think consumers are in fact willing to spend a little more on secure devices, but only if they are able to tell the difference. As it stands today, it is basically impossible for a consumer to look at two devices on the shelf, or at their Amazon listings, and make an informed assessment that one is more secure than the other. Product marketing rarely contains information like what kind of encryption and secure protocols are used, where the software is developed, where customer data is stored, whether a device will receive security updates, and so forth. And even if it did have such information, consumers would not be able to make heads or tails of, or care about, most of it. It's technical mumbo jumbo to everyone but software engineers, and the consequences of being hacked or having your data in the hands of Chinese intelligence seem hypothetical and distant, especially compared to the visceral attraction of a lower price today.

But to be clear, the threat to the country is anything but hypothetical, because wireless networking is increasingly in everything. As Bruce Schneier put it in his unsettlingly-named book *Click Here to Kill Everybody,* saying "I'm going on the Internet" makes as much sense as plugging in a toaster and saying, "I'm going on the power grid." It is hardly lost on manufacturers that some of the most successful tech businesses treat data as crown jewels; everything from wrenches to washing machines is going smart as fast as old equipment can be depreciated.

Attacks on unpatched devices are becoming more frequent and more dangerous. That was bad enough when we were talking about hacks on desktop computers, but a recent FBI advisory warned of increasing cyberattacks against unpatched medical devices. Unpatched industrial control systems threaten the availability of critical infrastructure. The Mirai botnet, which at its peak consisted of over 600,000 compromised devices performing large-scale cyberattacks in unison, grew by scanning the internet for devices with unpatched vulnerabilities, like IP cameras and routers, and taking control of them. And we have not yet seen the worst. An attacker could use unpatched vulnerabilities to take control of large numbers of mobile phones, turn their radios into signal jammers, and take down mobile networks. Botnets of commandeered high wattage devices like air conditioners, water heaters, and ovens could be used to disrupt the power grid and even cause large-scale blackouts. And attacks on cyberphysical systems like automated cars, or on medical devices, can directly cause widespread property destruction, human injury, and death.

Addressing this problem with a light regulatory touch is the promise of the FCC's Cyber Trust Mark program, a labeling program much like EnergyStar or USDA meat grades but for the security of connected devices. The way this will work is that as a device manufacturer, you certify that your device meets a list of cybersecurity criteria, such as that you use modern secure communications protocols and implement secure authentication, and in exchange, you get to put a flashy US Cyber Trust Mark logo on your packaging and sales materials, effectively an endorsement from the federal government of the security of your product. In addition to the moral and persuasive authority of the federal government on such issues, the true value of the mark will probably come from organizations, including the federal government itself, adopting the mark as a requirement for their procurement of connected devices.

The program is still in the works, and there is no guarantee the FCC gets it right. The Commission is under immense pressure from manufacturers to make the Cyber Trust Mark easy to earn. In one misguided vision of the program, success is measured by the number of manufacturers who have earned Cyber Trust Marks for their products within a few years of its inception. But given how dismal the cybersecurity landscape is right now, criteria that at most require minimal changes to what most manufacturers are already doing is clearly not enough. We don't lower the standard for USDA Prime to make sure that more cuts of meat qualify for it, and we shouldn't set the bar low for a federal government endorsement of a device's security.

I want to talk specifically about two criteria that I think are essential for the US Cyber Trust Mark to have teeth.

First, the program cannot merely be a checklist of specific security features that a product must have. If security could be reduced to a checklist, it wouldn't be such a continuing problem. Do you think that if there was some simple list of criteria for good security, that the most sophisticated organizations in the world would still continuously find themselves compromised by attacks on their internet-connected devices? They, and their insurers, would have adopted those criteria as requirements long ago, and major cyber intrusions would be a thing of the past. But that's not the world we live in. Which is not to say that lists of criteria cannot have utility. Many, such as the Federal Processing Information Standards (FIPS,) are respected by many organizations and do represent a good list of best practices, but they have nonetheless failed to stem the rising tide of vulnerabilities.

Instead, the program should require that manufacturers put skin in the game. In order to qualify for the mark, they should have to make legally enforceable promises to consumers that they have made a reasonable effort to develop a secure product and that they will continue to take such efforts, specifically by diligently identifying and patching vulnerabilities as they are discovered, for at least a period of time they commit to up front and advertise along with the device. The principle here is simple: the government has no business giving a cybersecurity endorsement to a manufacturer who puts devices on the market and then promptly abandons them, refusing to patch even glaring vulnerabilities that put their customers at risk. If a manufacturer that receives the trust mark fails to live up to that promise, it should be held liable in court, the same way we hold manufacturers liable in tort for defective products that maim or kill people. And, equally, manufacturers should not be subject to an open-ended liability regime under which they must perpetually support obsolete products. Consumers and enterprise users need to pay attention to support schedules and build equipment updates into their planning.

Second, manufacturers should have to disclose the jurisdictions in which the software that controls a device is developed, where software updates will be developed and deployed from, and where data collected by the device will be stored. Right now, consumers, businesses, and government agencies trying to avoid buying a trojan horse cannot easily access this information. For instance, even if a device is built in the US, if might have a cellular interface module or other component running Chinese-developed firmware, or receiving Chinese-deployed updates, or it may store sensitive user data in Chinese datacenters. To achieve digital

sovereignty over this or other suspect jurisdictions, and to protect our critical infrastructure from sabotage, we need to be able to easily rule out these devices for at least certain uses.

If we do a good job designing this program, then many manufacturers may decline to pursue a Cyber Trust Mark at first. That's fine. When you set a high bar, not everyone will be able to meet it right away. But by making the mark a requirement for procurement by the government and its contractors, which is a development that anyone currently booking significant cyber risk will welcome, we can begin to foster an ecosystem of devices whose manufacturers are willing to take responsibility for the security of their products, and that foreign adversaries cannot easily compel to insert a backdoor.

So coming back to the broader point, I was an early adopter of the Internet myself, and I admit that I partook in some of that early idealism. Thankfully, I don't think we have to give up that vision altogether. The Internet remains an incredible engine for commerce and the exchange of ideas. It still presents one of the greatest obstacles to censorship ever created. But it's becoming impossible to avoid contending with the sober realities of international political, legal, and military conflict. Thank you for your attention. I look forward to taking any questions you may have.