Hearing Before the Subcommittee on Crime and Terrorism,
U.S. Senate Committee on the Judiciary
"How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors"
November 5, 2019

Responses to Questions for the Record
Tom Burt
Corporate Vice President of Costumer Security and Trust
Microsoft Corporation

QUESTIONS FROM SENATOR BOOKER

1. In March 2019, court documents were unsealed showing that Microsoft had successfully brought legal suits to take down 99 phony websites that were used in a years-long "spear-phishing" campaign to steal customers' information.[1] As you noted at the time, the threat group's activities targeted "businesses and government agencies," as well as "activists and journalists—especially those involved in advocacy and reporting on issues related to the Middle East."[2]

    a. During your testimony, you emphasized that Microsoft views public-private partnerships in the cybersecurity field as particularly important. What was the nature of the role, if any, played by the federal government in helping you to bring these suits to court?

Microsoft Response: The federal government had a very limited role in our action against Phosphorus (the action referenced in the question) or other nation-state court actions we have filed. In some instances (e.g., actions we filed against Barium, a nation-state actor operating from China) we have subsequently referred cases to U.S. law enforcement for possible criminal action. We would like to engage in more coordinated disruptions and to build a stronger strategic relationship with the intelligence community so that the work we do to protect our customers can be, when possible, complimentary of the work being done by the federal government or our allies to target the same actors. We have discussed this approach but have more work to do.

    b. Microsoft argued in this litigation that the threat group was violating the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, as well as engaging in trademark violations. One commentator praised this effort as the kind of "creative lawyering" needed for companies to do more than play defense on

[1] Ellen Nakashima & Spencer S. Hsu, *Microsoft Says It Has Found Iranian Hackers Targeting U.S. Agencies, Companies and Middle East Advocates*, WASH. POST (Mar. 27, 2019), https://www.washingtonpost.com/local/legal-issues/microsoft-says-it-has-found-iranian-hackers-targeting-us-agencies-companies-and-middle-east-advocates/2019/03/27/8056c51e-50a0-11e9-8d28-f5149e5a2fda_story.html.

[2] Tom Burt, *New Steps To Protect Customers from Hacking*, MICROSOFT (Mar. 27, 2019), https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking.

cybersecurity.[3] What strategic benefits does federal litigation offer for combating this type of illicit cyber activity?

Microsoft Response: This civil litigation strategy was pioneered by our Digital Crimes Unit to disrupt the activities of criminal botnets. We first used this approach in the nation-state context to target Strontium, a nation-state actor operating from Russia, also known as APT28/Fancy Bear. Civil litigation involves the strategic benefits of speed and flexibility to address threats that are scaled and dynamic. The federal courts' broad and flexible equitable powers to issue injunctions are effective because they can address the nature of cybercriminals' technical architecture and court orders can evolve as the cybercriminals change their methods of operation. In the Strontium case we were able to use the Special Master provisions of the federal rules of civil procedure to establish a post-judgment process to enable rapid take down of adversary infrastructure; being able to respond to adversaries with speed and agility is key to successful disruption. Court orders can also ensure in appropriate cases, that mitigation occurs quickly and in a coordinated fashion through third-party infrastructure providers that are involved.

Civil litigation allows Microsoft to stop the harm, notify the victims through work with internet service providers (ISPs) and remediate the threat. The civil rule behind Microsoft's key legal strategy (Fed. Rule Civil Proc. 65) was crafted by Congress to address damages similar to those confronting cyber-crime victims today in that it seeks to immediately stop the harm to victims even before a hearing takes place.[4] It is this emphasis on stopping victim harm which differentiates federal civil action from criminal prosecution. Criminal actions primarily focus on attribution and the deterrent impact resulting from arrest and criminal conviction. But in most cases the individuals responsible for nation state actions will be outside effective criminal jurisdiction – but their activities within the U.S., and the flexible forms of notice provided under the federal civil rules, enable us to take action to disrupt adversary infrastructure without the physical presence of the human actors in the U.S.

Additionally, Microsoft filed federal civil actions against unknown defendants through the use of a "John Doe" suit. This procedural tool has traditionally been used to maintain a statute of limitations when there is some uncertainty as to the exact identity of the parties involved, but there is sufficient evidence to support a *prima facie* claim against the unknown parties. Using this type of action in a cybercrime case has allowed us to take immediate action against the criminal infrastructure to protect victims and stop the harm first while subsequently leveraging the concept of "Doe" discovery to attempt attribution. By leveraging "Doe" discovery in its civil litigation, Microsoft's Digital Crimes Unit has been successful in identifying several individuals that have been referred to law enforcement. This same approach, again, is useful in the context of nation-

---

[3] Joseph Marks, *The Cybersecurity 202: Microsoft's Takedown of Iranian Fake Sites Shows 'Creative Lawyering,' Experts Say*, WASH. POST (Mar. 28, 2019), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/28/the-cybersecurity-202-microsoft-s-takedown-of-iranian-group-shows-creative-lawyering-experts-say/5c9c19c11b326b0f7f38f292.

4 **Rule 65. Injunctions and Restraining Orders**

(b) Temporary Restraining Order.

(1) Issuing Without Notice. The court may issue a temporary restraining order *without written or oral notice to the adverse party* or its attorney only if:

(A) specific facts in an affidavit or a verified complaint clearly show *that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition*; and

(B) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required.

state attackers, when a great deal is known about the techniques used by the attacker, and their victims, but the information available to us does not enable identification of specific individuals.

c. What steps can the federal government take to help companies like Microsoft protect consumers from similar spear-phishing schemes?

Microsoft Response: The government could use technical and legal operations to disrupt spear-phishing infrastructure as soon as it is created through civil legal authorities similar to those used by Microsoft. The government could also use *in rem* actions, at scale, against the infrastructure and tools utilized, including but not limited to, actions to address systemic domain abuse. Microsoft would also like to continue to collaborate with the government when legally appropriate in the mutual exchange of technical threat data. Appropriate data sharing provides better visibility to the private sector and government alike, and better opportunities for prompt mitigation and disruption of threats. Information on trends and investigations into criminal organizations which have been identified as leveraging private sector services and infrastructure would assist investigations and allow for the disruption of spear-phishing campaigns and the implementation of technical countermeasures. The government can also prioritize the efforts being led by the Justice Department to quickly conclude new Cloud Act agreements.

2. During your testimony, you said that Microsoft's digital crimes unit is "truly unique in the private sector, combats business email compromise crime and continues to lead the world in our efforts to shut down criminal botnets." You also stated that Microsoft, "[w]orking closely with law enforcement and private sector partners," has "taken down 17 botnets, rescuing close to 500 million devices from these criminal networks."[5]
    a. Can you provide any further detail about the specific capacities, or at least the nature of the efforts, in which Microsoft has worked with law enforcement to shut down criminal botnets?

Microsoft Response: For many years Microsoft has worked with law enforcement in cases involving multi-jurisdictional cyber-crime to coordinate the seizing of domains, command and control servers, and other criminal infrastructure. In the most successful actions this has been done contemporaneous with an indictment. In fact, our initial actions were so successful that we saw a dramatic shift in the cybercriminal's methodology around 2012, when they began dispersing their infrastructure throughout the world in an effort to hamper any coordinated disruption on the part of either private or public entities. We continue to work closely with U.S. and foreign law enforcement to provide forensic evidence identifying criminal infrastructure as we prepare our civil strategy to disrupt criminal botnets. We believe that the trend towards further dispersion and obfuscation of cyber-crime infrastructure will grow in the coming years and with it the need for better coordination and communication between the private and public sectors on a global scale. We look forward to improved collaboration with law enforcement in the U.S. and globally to achieve these goals.

b. In your assessment, what unique advantages does Microsoft's digital crimes unit possess that make it a particularly effective private sector partner for law

[5] *Senate Judiciary Subcommittee on Crime and Terrorism Holds Hearing on Data Security*, CQ CONG. TRANSCRIPTS (Nov. 5, 2019), https://plus.cq.com/doc/congressionaltranscripts-5765095.

enforcement?

Microsoft's Digital Crimes Unit (DCU) has been and continues to be a unique asset within the tech industry. Our objective is to bring Microsoft's unique assets to bear in protecting our customers from the growing threat of cybercrime. One of the fundamental attributes of the DCU is our cross disciplinary approach to tackling cyber-crime problems. DCU's cyber investigators excel in the complex process of analyzing complex criminal cyber-crime infrastructure and our data analysis team applies machine learning, AI and data visualization technology in creative ways to identify criminals not understand criminal activity, all while leveraging Microsoft's multiple security groups and their technical expertise. This provides us with an unprecedented ability to react quickly to new threats targeting our customers. The DCU attorneys' deep understanding of both criminal and civil litigation, as well as privacy laws, allows DCU to investigate and prepare complex cyber-crime cases for civil litigation and criminal referrals. We have developed a strong and trusted relationship with key law enforcement agencies globally. We also try to move quickly as criminals are constantly changing their network and moving their infrastructure.

c. In your experience, has law enforcement lacked statutory authority in any specific areas to enable it to work effectively with Microsoft or other private sector entities in shutting down criminal botnets or combatting business e-mail compromise crimes?

Microsoft Response: Microsoft believes that U.S. law enforcement generally possess both civil and criminal statutory authority to combat cyber-criminal networks, however, there is always the possibility of improvement. Before any statutory change is made the traditional objectives in addressing crime and criminal networks need to be reviewed to address the different nature of cybercrime. For example, a focus on arrest and prosecution could result in a lack of focus on disruption and dismantlement of botnets – and thus the protection of current and future victims -- because, in large part, there is not a readily identifiable person(s) to prosecute – even where ongoing crimes are being committed. Cybercrime and nation-state attacks are also almost always global activities. Therefore, the ability of law enforcement agencies to obtain information across borders in an efficient way that observes core legal and human rights principles is essential. This is why Microsoft supported the passage of the CLOUD Act by Congress and advocates for increased focus by government on conclusion of CLOUD Act agreements with countries around the world.

3. A senior advisor at the National Institute of Standards and Technology (NIST), Naomi Lefkovitz, recently stated that NIST will likely publish the first version of its Privacy Framework, which is intended to help organizations manage privacy risk, by the end of this year.[6] NIST reportedly received suggestions from more than 50 organizations and a dozen individuals on how to refine this privacy framework, which builds on NIST's Cybersecurity Framework from 2014.[7]

a. Did Microsoft offer suggestions to NIST in the development of the Privacy Framework? If so, can you describe the nature of Microsoft's input?

[6] Eric Chabrow, *Getting Ready for the NIST Privacy Framework: NIST's Naomi Lefkovitz Offers Insights on How to Use the Framework*, BANKINFOSECURITY (Nov. 6, 2019), https://www.bankinfosecurity.com/interviews/getting- ready-for-nist-privacy-framework-i-4497.
[7] *Id.*

Microsoft Response: Yes, Microsoft participated in the development of the NIST Privacy Framework. We recommend that the NIST Privacy Framework be consistent with existing privacy laws. Consistency with U.S. and international privacy laws will enable companies to more readily implement the Framework. Our high-level recommendations were that the Privacy Framework:

- Be interoperable with leading privacy regimes. This helps better protect citizen's private data, promotes global commerce and reduces operating costs for meeting privacy obligations.
- Be forward looking. The Privacy Framework should be flexible to address changes in technologies and policies over time.
- Be risk-based and outcome-focused. Implementation of good privacy practices for any organization should start with a rigorous and documented risk-assessment which then establishes mitigations such that the benefits of processing personal data outweigh the residual risks.
- Have an explicit and complimentary relationship to the NIST Cybersecurity Framework. This will encourage organizations to more easily integrate security and privacy operations.

The NIST Privacy Framework has progressed well over the past year and Microsoft continues to contribute substantive comments to improve the framework for practical implementation. Additionally, Microsoft has consistently encouraged NIST to incorporate relevant international standards (such as the Privacy Information Management System – ISO/IEC 27701) and to be flexible enough to map to emerging laws and policies.

b. During your testimony, you stated that the current NIST Cybersecurity Framework is, "very complex" and "can be hard to implement" for companies that "don't have a big IT staff."[8] What kinds of steps could NIST take to revise its framework so that smaller companies can more readily implement these measures?

Microsoft Response: Microsoft encourages NIST to offer guidance tailored to specific sectors or types of organizations based on risk appetite, resources, and level of expertise. To complement broader efforts, NIST might also consider providing guidance on how the use of new technology, such as cloud computing, could help small businesses facilitate more streamlined implementation of cyber risk management.

Though the Cybersecurity Framework currently represents a helpful cross-sector baseline for security, as with many areas of risk management, a one-size-fits-all approach is insufficient. Organizations often need more tailored guidance, to help them focus on what's most critical to them or scale up risk management practices over time. To help adapt, certain sectors developed "profiles"-- including the financial services sector, manufacturing sector, and smart grid providers within the energy sector. As suggested in section 2.3 of the Cybersecurity Framework, some organizations developed even more unique profiles for their own operations, capturing their current and target profiles for cyber risk management readiness and intended investments and security outcomes.

NIST has acknowledged the potential value of a profile – or multiple profiles – for the small business community. In its Cybersecurity Framework Roadmap, NIST states that it will further

[8] *Senate Judiciary Subcommittee on Crime and Terrorism Holds Hearing on Data Security*, CQ CONG. TRANSCRIPTS (Nov. 5, 2019), https://plus.cq.com/doc/congressionaltranscripts-5765095.

amplify small business awareness of cybersecurity by developing small business Cybersecurity Framework "starter profiles" tailored toward risk management of business processes important to small business owners. Given that developing a Framework profile can be an intensive process, NIST's development of profiles for small businesses would likely help small business more readily leverage the Framework and drive implementation of the Framework's security measures. Rather than changing the entire Cybersecurity Framework, which is currently applicable across many sectors and business scenarios, for a particular community, this sort of tailoring activity would be a valuable addition.

More broadly, NIST has given attention to this issue by developing materials that complement the Cybersecurity Framework and specifically target smaller companies. For instance, it developed NISTIR 7621: Small Business Information Security: The Fundamentals. NIST has also organized materials that have been developed to help small businesses understand the Framework or better protect their organizations through guidance or tools that are narrower in focus – on the Framework site and as part of NIST's recently launched Small Business Cybersecurity Corner. There are also numerous efforts that leverage the Cybersecurity Framework as a starting point in developing guidance for small businesses, including the National Cyber Security Alliance's CyberSecure My Business program and the Cyber Readiness Institute's Cyber Readiness Program.

4. International initiatives such as the Paris Call for Trust and Security in Cyberspace have sought to make countries voluntarily commit to various cybersecurity principles. As you noted in your testimony, "the Paris Call has been endorsed by more than 65 governments and over 500 enterprises and organizations. Unfortunately, the United States has not yet endorsed the Paris Call."[9]

    a. From your own perspective, have the governments that have supported the Paris Call begun making concrete progress toward the nine cybersecurity goals outlined in the Paris Call?

Microsoft Response: As of November 12, 2019, the one-year anniversary of the Paris Call for Trust and Security in Cyberspace, there are now 74 national government endorsements for the agreement and over 1,000 total supporting entities from across stakeholder groups. This is the largest ever multi-stakeholder cybersecurity agreement of its kind. The newly launched website for the Paris Call has begun cataloguing multi-stakeholder initiatives to support the respective principles of the agreement. For Microsoft's part, we are working with the Alliance for Securing Democracy to build a community of partners – including members of government, industry and civil society – to improve capacities to prevent election interference, in accordance with the third Paris Call principle.[10] Other initiatives include "bug bounty" programs to limit the proliferation of malicious cyber exploits, the Carnegie Endowment's recommendations on ICT supply chain security, and the Organization of Security Cooperation in Europe's (OSCE) work to establish points of contact across its member states to share information about cyber incidents.[11] We expect to see further growth in these collaborative efforts among Paris Call supporters over the second year of the agreement, which would be all the more impactful with

[9] *Id.*
[10] *The 9 Principles*. Paris Call for Trust and Security in Cyberspace Website. French Ministry for Europe and Foreign Affairs. https://pariscall.international/en/principles
[11] Ibid

the participation, support and leadership of the United States behind it.

Encouragingly, governments are taking concrete action in accordance with these principles, particularly in the European Union. For example, the EU's Network and Information Security (NIS) Directive[12] includes requirements for protecting critical infrastructure, and the recently-established EU sanctions regime for cyberattacks[13][14] discourages actions that can harm infrastructure, elections systems, and intellectual property – all of which are protected categories specifically enumerated in the Paris Call. Meanwhile, the Organization of American States (OAS) – of which eleven members are Paris Call supporters – recently agreed to a set of four confidence building measures to "Promote Cooperation and Trust in Cyberspace,"[15] another form of interstate collaboration highlighted in the Paris Call. In addition, the Australian government released a publication in September outlining how they are implementing their international commitments in cyberspace.[16] While there are certainly many more examples of state activities in line with the nine principles, the Paris Call itself importantly also establishes a broad platform to support cooperative initiatives among its endorsers across all stakeholder groups.

b. Do you believe that the United States' failure to support the Paris Call hinders the development of international cybersecurity norms?

Microsoft Response: United States leadership remains indispensable in the international system, especially in setting expectations for behavior in cyberspace. As the Paris Call is based largely on principles that were originally spearheaded by the United States in other forums, it presents a unique opportunity for the U.S. to see its own priorities in cyberspace advanced by a growing community of stakeholders around the world. And while the work of the Paris Call will continue in the absence of support from the United States Government, an endorsement for the agreement would be consistent with U.S. security priorities and invaluable to developing and recognizing international cybersecurity norms to increase trust, safety, security and stability online.

Notably, among the government supporters of the Paris Call are most of the United States' major allies – including the entirety of the EU, every other "five-eyes" nation, and all other members of the NATO alliance except Turkey. And while the United States has yet to give its support to the agreement, the nine voluntary Paris Call principles are largely based on cybersecurity norms the U.S. has led in establishing at the United Nations and in other multilateral forums (*see Chart 1 below*). This multi-stakeholder affirmation of the rules and norms that the U.S. has erstwhile championed reflects how these essential expectations can

[12] *Nis Directive.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/nis-directive
[13] *Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.* EUR-Lex. http://data.europa.eu/eli/dec/2019/797/oj
[14] *Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.* EUR-Lex. http://data.europa.eu/eli/reg/2019/796/oj
[15] *Regional Confidence-Building Measures (CBMS) to Promote Cooperation and Trust in Cyberspace (Approved at the fourth plenary session held on May 24, 2019)*. Organization of American States. May 24, 2019. http://scm.oas.org/doc_public/ENGLISH/HIST_19/CICTE01297E03.doc.
[16] *Australian Paper – Open Ended Working Group on developments in the field of information and telecommunications in the context of international security.* Australian Mission to the United Nations. Sept. 2019. https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf

and are taking hold and gaining the necessary recognition to have real impact.

The importance and potential of the Paris Call is further underscored by the growing number of state and local governments in the U.S. that have joined onto the agreement even in the absence of support from the federal government. This includes endorsements from the states of Colorado, Virginia, and Washington, as well as the cities of San Jose and Louisville.[17] Municipalities across the country, in particular, are desperate for more action to be taken to establish clear rules and boundaries for behavior in cyberspace as high profile ransomware attacks have crippled the operations of many city governments and authorities in the U.S. in recent months.[18] We hope this support by state and local authorities can serve as a clarion call to the federal government to stand alongside them, and so many others across the world, in supporting the principles and multi-stakeholder approach of the Paris Call.

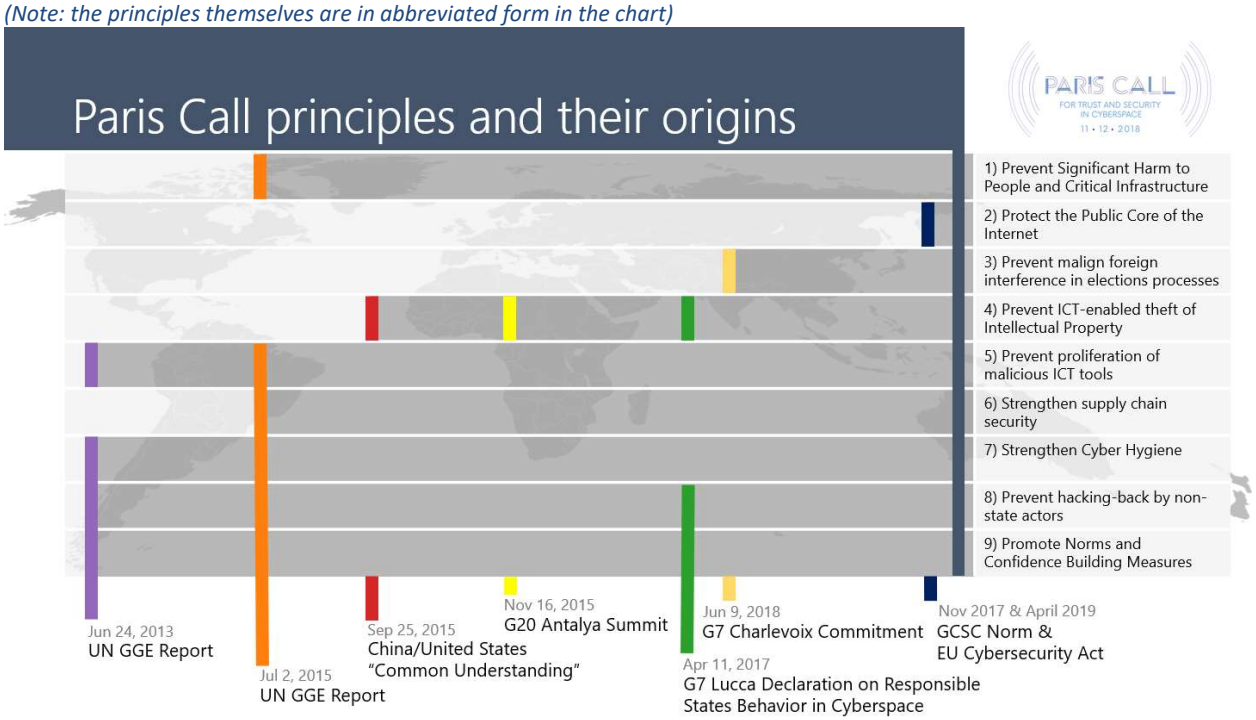
Cyberspace is distinct from the physical domains of conflict in that the infrastructure and systems which maintain it are largely owned and operated by the private sector. As a result, meaningful norms and rules for responsible behavior online require the input and often support of a broader multi-stakeholder coalition. This is what makes the Paris Call such a promising initiative – as it includes members of industry, civil society and the public sector alongside national governments. This type of coalition has the potential to not only establish norms for cyberspace, but to promote and reinforce them across stakeholder groups to ensure they are upheld. Indeed, it is unclear how norms developed in other forums are expected to be progressed in the absence of such an agreement, which includes the actors from different sectors that will be responsible for implementing and adhering to these voluntary but essential expectations.

This is not to dismiss the value of more traditional multilateral forums for cybersecurity norms development, such as those at the United Nations. In fact, there are presently two parallel dialogues taking place at the UN that would benefit greatly from forward leaning U.S. leadership. The UN Group of Governmental Experts (UNGGE) and the Open Ended Working Group (OEWG) on "information security" have each begun their deliberations and consultations this fall, creating opportunities to further establish meaningful rules of the road for cyberspace. As a participant in both these dialogues – and the driving force behind establishing the UNGGE – the U.S. could advance greater stability in cyberspace by helping facilitate the inclusion of essential multi-stakeholder input and by promoting the implementation and enforceability of international norms for responsible state behavior in cyberspace as key objectives in these discussions.

[17] Marks, Joseph. *The Cybersecurity 202: States and cities make cybersecurity pledge after Trump administration rejects it.* The Washington Post. Nov. 15, 2019. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/11/15/the-cybersecurity-202-states-and-cities-make-cybersecurity-pledge-after-trump-administration-rejects-it/5dcd8c2388e0fa10ffd20e7d/

[18] Sanger, David, Manny Fernandez, Marina Martinez. *Ransomware Attacks Are Testing Resolve of Cities Across America*. The New York Times. Aug. 22, 2019. https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html

Chart 1: Paris Call principles reflected in previous international agreements
(Note: the principles themselves are in abbreviated form in the chart)



5. One of your fellow witnesses, William Cater, said during his testimony that "policies like data localization, encryption mandates and data retention requirements that companies are pursuing to preserve their access to data can lead to worse security outcomes for everyone."[19]

    a. Do you agree that data localization can lead to worse security outcomes?

Microsoft response: Microsoft understands "data localization" to refer to keeping certain data and functions associated with data within a particular country. Whether data localization leads to worse security outcomes depends on the nature and the extent of the data localization across three variables. These variables are the scope of data (e.g., some data or all data), the types of data processing (e.g., all data processing or just storage), and the rule of law applicable to access to and use of the data by the applicable government or other actors.

The requirement merely to store limited data, such as personal data or certain types of industry data, within a particular country does not by itself lead to worse security outcomes for the U.S. government or for users of technology. In this scenario, the US government and technology companies still would have full access to information on cybersecurity threats and be able to respond accordingly. But to the extent that such a requirement would enable access to and use of the data of U.S. enterprises or individuals by another government or those acting on its behalf, the security of the data itself could be more greatly threatened by such requirements.

[19] *Id.*

In addition, data localization that requires all data to be processed, transited, and stored exclusively within a particular country would lead to pockets of isolation. This "Balkanization," as some have called this type of factious isolation, can lead to worse security outcomes for both the U.S. government and for consumers because it would hinder the ability of the U.S. government and the private sector to access cybersecurity threat intelligence, respond to cybersecurity threats expeditiously, and update technical security measures to keep up with emerging threats.

b. Absent data localization, how can the United States protect its data from countries that do not share its values?

Microsoft Response: By itself, data localization does not lead to better security outcomes and can, if taken to an extreme, actually lead to worse security outcomes. The U.S. can protect its data by continuing to exchange cybersecurity threat intelligence with the U.S. private sector; establishing cybersecurity standards beyond the NIST Cybersecurity Framework so that small and medium-sized companies could implement cybersecurity controls more easily, adopting and using technology with advanced security that can prevent security incidents and respond to evolving threats, and by joining the Paris Call and taking other steps to advance norms and rules of conduct by governments in the cyber domain.

6. Location data can reveal sensitive information about American consumers. For example, as a *New York Times* investigation found last year, "[a]t least 75 companies receive anonymous, precise location data from apps whose users enable location services to get local news and weather or other information," and "[s]everal of those businesses claim to track up to 200 million mobile devices in the United States." While "the information apps collect is tied not to someone's name or phone number but to a unique ID," the report continued, "those with access to the raw data—including employees or clients—could still identify a person without consent."[20] Another report, by *Vice*, found that bounty hunters could purchase the current location of a mobile phone for $300.[21]

a. What safeguards does Microsoft place on the collection and use of location data through its own products?

Microsoft Response: Microsoft treats precise location data as sensitive customer data. For Microsoft products and services that use location data, Microsoft requires an explicit consent to collect such data and for that data to be used for a particular purpose. When location data is collected, Microsoft further safeguards customers by providing customers with the ability to view, edit, export and delete the precise location data that is processed by Microsoft. For Windows 10 device users, if the customer has enabled the device location setting, the device sends de-identified location information to Microsoft after removing all personally identifiable information at the device. Microsoft does not sell customer location data or location inferences collected from Microsoft products to third parties. Additional information regarding how Microsoft safeguards

[20] *Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Kroli, Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.*

21 Joseph Cox, I Gave a Bounty Hunter $300. Then He Located Our Phone, VICE (Jan. 8, 2019), https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

customer location data can be found here: https://support.microsoft.com/en-us/help/4468240/windows-10-location-service-and-privacy

b. At a broad level, how concerned are you that hackers, cybercriminals, or foreign adversaries could access and misuse Americans' location data, and what forms could such abuses take?

Microsoft Response: Privacy and security are important to Microsoft and we ensure that location data is stored in accordance with industry standard information security practices. When location data is stored on a user's device, the security practices are subject to the device security.

Hearing Before the Subcommittee on Crime and Terrorism,
U.S. Senate Committee on the Judiciary
"How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors"
November 5, 2019

Responses to Questions for the Record
Tom Burt
Corporate Vice President of Costumer Security and Trust Microsoft Corporation

QUESTIONS FROM SENATOR BLUMENTHAL

1. In 2004, Skype — then owned by eBay — announced a joint venture with TOM Online, a Chinese internet company, to launch a Chinese-language version of Skype. However, human rights activists and reporters soon discovered that Skype was censoring certain words in user messages, such as "Dalai Lama." Reports also suggested that the Chinese government was using Skype to spy on its users. In 2011, Microsoft acquired Skype and, two years later, terminated the joint venture with TOM. Microsoft then implemented new encryption measures to protect the messages and accounts of Chinese users. The Skype app was pulled from Apple's App Store in China in November 2017.

    a. Did the Chinese version of Skype, TOM-Skype, censor the communications of its users? If so, what was the nature of that censorship? Please be specific.

Microsoft response: Yes. TOM operated a text filter that blocked the sending of messages containing terms deemed sensitive by the Chinese government. As noted in the question, Skype and TOM entered into a joint venture and those terms were in place prior to Microsoft's acquisition of the company.

    b. Did TOM-Skype allow the Chinese government to listen in to the chats and calls of its users? How did the Chinese government access these communications?

Microsoft response: We do not know whether the Chinese government was able to listen in to the chats and calls of TOM-Skype users.

    c. Was Microsoft in control of what TOM was doing with the Chinese Skype client? Did Microsoft cut ties with TOM based on these issues?

Microsoft response: Microsoft was not in control of what TOM was doing with the Chinese Skype client. Microsoft terminated its relationship with TOM in 2013.

As media reported at the time, Microsoft and its new partner for Skype in China implemented encryption to protect the privacy of users and their communications.[1]

d. Who was responsible for the new, more-secure Skype app being pulled from Apple's Chinese App Store? Did Apple or the Chinese government provide you notice or demands prior to pulling down the app?

Microsoft response: Microsoft received a notice from Apple in October 2017 indicating that Skype was removed from the China App Store because Skype did not have telecommunication licenses required to operate in China.

In November 2017, Apple stated the following about the removal of Skype from the App store:

> "We have been notified by the Ministry of Public Security that a number of voice over internet protocol apps do not comply with local law. Therefore these apps have been removed from the app store in China."[2]

e. Do you have any recommendations to ensure companies are not tempted to make commitments that put Americans or our national interest at risk?

Microsoft response: Microsoft stands for using technology to defend democratic values. Doing business globally is complex, but we have taken an approach that puts democratic values first and foremost. This includes our full commitment to doing our part to safeguard U.S. national security.

2. Chinese hackers carry out massive campaigns to steal intellectual property and trade secrets from U.S. companies, amounting to billions of dollars of losses to our economy. In 2015, the Obama administration was prepared to exercise an executive order that would authorize sanctions against companies or individuals that profit from this cyber theft, including state-owned enterprises and senior Chinese officials.

Using the threat of U.S. sanctions, President Xi Jinping and President Obama agreed that neither of their countries would "conduct [nor] knowingly support cyber-enabled theft … including trade secret or other confidential business information." After they reached this agreement, cybersecurity companies recorded a steep decline in Chinese attacks against U.S. companies that continued into 2016. However, in the past three years, cybersecurity companies have reported Chinese hackers have resumed their campaigns.

a. Microsoft does a considerable amount of work tracking foreign hacking campaigns. Did the agreement between the Obama Administration and China

[1] Paul Carsten, "Microsoft Blocks Censorship of Skype in China: Advocacy Group," *Reuters,* November 27, 2013. https://www.reuters.com/article/us-microsoft-china-censorship-idUSBRE9AQ0Q520131127

[2] Paul Mozur, "Skype Vanishes from app stores in China, including Apple's," *New York Times*, November 21, 2017.

decrease Chinese intellectual property theft and economic espionage?

Microsoft response: The general experience of our analysts in the Microsoft security community was that there was indeed a decrease in Chinese hacking of US companies following the agreement reached between China and the United States in 2015. While we did not publish any findings at that time, others in the community did, and those remain useful data points to help inform discussions about the value of diplomacy in reducing cyberattacks.

b. Has Microsoft seen an increase in Chinese intellectual property theft and economic espionage in the past three years?

Microsoft response: What was distinct about the attacks in 2015 coming from China was their overtness. While attacks have continued, the tactics used are less overt, and can be harder to detect. We do not track attacks through modalities like intellectual property theft or economic espionage, and thus do not have data to address this question.

3. U.S. intelligence and law enforcement agencies have warned that Russia, Iran, and others have sought to interfere in the 2020 presidential campaigns using disinformation and hacking. Until recently, China has been less visible about using Facebook and Twitter to meddle in our political affairs. This is despite the Chinese Communist Party's considerable success at shaping public opinion at home, thanks to a blend of online censorship, patriotic trolls, and directives to state-run media.

a. Has Microsoft seen any evidence that China has targeted U.S. politicians or political campaigns, whether for purposes of disinformation or espionage? If yes, please cite direct examples.

Microsoft Response: Microsoft has not observed any cyber attacks against US politicians or campaigns at this time.