REVIEW OF STRATEGIC APPROACHES

Option 1: Disavow Legislation and Other Compulsory Actions

Engagement Strategy and Timeline

- September: Outreach to foreign allies to signal our strong resistance to efforts to compel access; outreach to U.S. industry, the technology community, and civil society to coordinate messaging; attempt to convince other allies to come out with a similar statement at the same time.

- October: The President issues a statement strongly disavowing legislation or other efforts to compel access and calling on U.S. industry to resist efforts by other nations to compel access; coordinated industry and civil society statements of support; coordinated foreign partner statements of agreement.

- November: Outreach to other governments to bring more allies in alignment with our position; outreach to U.S. industry to build voluntary cooperation in the absence of compulsion; host public discussions and debates on encryption policy with U.S. industry and foreign allies.

Top Line Message

- The problem of criminals using strong encryption to frustrate law enforcement's information gathering is a real and growing problem but we have not found a secure, practical solution.

- People around the world rely on the security of U.S. products and services in their daily lives. Mandating the design of those systems to include known vulnerabilities makes all of us less safe and undermines trust in these digital services.

- It is critical that law enforcement be able to access the information that it needs to protect public safety and national security. We will continue to use all of the tools available to us lawfully to keep American citizens safe.

- Overall, the benefits to privacy, civil liberties, and cybersecurity gained from encryption outweigh the broader risks that would have been created by weakening encryption.

- Accordingly, the Administration will not seek legislation that compels providers to design their products to enable

government access to encrypted information, even pursuant to lawful process.

- We expect that foreign governments will also take a hard look at this difficult issue, and hope that they will come to the same conclusion. We call on U.S. industry to resist efforts by other governments to mandate such access.

Impact on Policy Equities

Public Safety and National Security. In the near term, this approach would not provide any relief to law enforcement efforts to counter the increasing use of encryption by criminals, including terrorists. As a result, the public safety drawbacks would be significant, though the precise extent of the drawback versus other proposals is unclear because bad actors will increasingly be able to frustrate law enforcement efforts to access their communications through lawful process. This approach would remove technology companies' most consistent grievance with the Administration, which could improve cooperation across a range of important priorities on technology issues including, but not limited to, encryption. It may also foster better cooperation on information that is not encrypted and will not fracture the Internet products and services market which may also preserve better access to unencrypted information, thus aiding public safety/national security.

Cybersecurity. Pro-encryption statements from the government could also encourage broader use of encryption, which would also benefit global cybersecurity. Further, because any new access point to encrypted data increases risk, eschewing mandated technical changes ensures the greatest technical security. At the same time, the increased use of encryption could stymie law enforcement's ability to investigate and prosecute cybercriminals, though the extent of this threat over any other option is unclear as sophisticated criminals will use inaccessible encryption.

Economic Competitiveness. This approach could help undercut foreign competitors' criticisms that U.S. companies' products are instruments of U.S. mass surveillance, and would clearly differentiate U.S. policy from moves by China and others to mandate decryption. However, if other markets do not follow our lead, and instead demand access, it is more difficult to assess the impact of this approach. On the one hand, U.S. companies could be forced to avoid those markets or develop access

solutions. On the other, the failure of some nations to follow the U.S. lead could bolster the reputation of the United States as a leading source of technically secure products and services.

Civil Liberties and Human Rights. Domestically, many privacy and civil liberties advocates would regard this approach as a significant step in defense of privacy and free expression around the world. If other nations follow our lead or companies successfully resist country demands, this approach could limit repressive regimes' willingness to demand access to encrypted information, which likely would help protect dissidents and other communities in danger of human rights violations.

Likely Reaction of Key Stakeholders

Industry and Civil Society. This sector would strongly support this approach.

Other Governments. Likely to be divided. This position would contradict the stated policy of some allies (e.g., the United Kingdom, France, and the Netherlands) who argue that governments should not allow "safe spaces" for extremists. As a result, those allies could criticize the U.S. position as endangering the safety of their citizens. Other foreign partners that are strong advocates for free expression online and have not argued for government access to encrypted information (e.g., Germany and Estonia) are more likely to support this approach.

Pros

- Some in industry have indicated that a strong statement disavowing legislation is a precondition to voluntary cooperation with the United States Government. Since the prospects of legislation are dim, this approach could help build cooperation without limiting broader policy options.

- Counters the narrative that the United States is seeking to expand its surveillance capability at the expense of cybersecurity, and could help repair trust in the United States Government and U.S. companies overseas.

- A strong statement from the United States could make it more difficult for authoritarian regimes to seek compulsory legislation, although working group participants are divided on whether adopting this approach would actually stop such calls.

- May weaken future calls for data localization since it will be harder for other countries to claim they are "protecting" their citizens' data from the United States.

- Could provide some positive benefit for U.S. negotiations on the U.S.-EU Data Protection and Privacy Agreement, Safe Harbor, and Transatlantic Trade and Investment Partnership.

- Is the strongest option for cybersecurity, economic competitiveness and civil liberties and human rights.

Cons

- This approach provides no immediate solution to the challenges that the expanding use of encryption poses to law enforcement and national security today and is the weakest option from that perspective.

- Some working group participants argue this approach would remove a key point of leverage - the threat of legislation - in our negotiations with industry (although few, if any, in industry likely find this threat to be credible).

- U.S. providers have not indicated they would be willing to voluntarily modify their systems to enable law enforcement access to encrypted information, even if the government were to eschew legislation, and could result in the United States being isolated in its position.

Option 2: Defer on Legislation and Other Compulsory Actions

This option could be pursued with two distinct goals in mind. Under option 2(a), the Administration would seek industry's voluntary assistance to modify their technology to address law enforcement's concerns. Under option 2(b), the Administration would accept the current status quo and not seek technical modifications, but would still ask providers to assist law enforcement in any way that they can within their current technological framework. In either case, these calls for assistance could be done publicly or privately, depending on the preferred engagement framework.

Engagement Strategy and Timeline

- September: Outreach to foreign allies to assess their positions; signal to allies that the United States does not think legislation is the right way forward at this time; work

with other governments to identify voluntary action by industry that would help to mitigate their concerns; outreach to U.S. industry to coordinate messaging.

- October: The President issues a statement disavowing legislation, but acknowledges the serious challenges posed by encryption for public safety and national security; secure coordinated statements of support or agreement from industry, civil society, and partner nations.

- October-November: Outreach to foreign allies in the wake of the statement to bring more allies in alignment with our position; outreach to U.S. industry to build voluntary cooperation in the absence of compulsion; if some allies persist in demanding access, consider whether the United States Government should highlight the difference in positions and the U.S. emphasis on privacy-protections.

- Post-November: Host public discussions on encryption policy with U.S. industry and foreign allies; should foreign allies demand and secure access, consider whether to call upon U.S. industry to provide the same access to the United States Government.

Top Line Message

- The United States is not seeking legislation at this time to compel providers to change their products to enable government access to encrypted information pursuant to lawful process.

- At this point, legislation appears neither feasible or easily draftable. We need considerable public discussion before we would be in position to contemplate a legislative solution.

- However, we also cannot ignore the barriers that inaccessible encryption can create to law enforcement's critical need to investigate and prosecute criminals, including terrorists - and the threat these barriers create for public safety.

Impact on Policy Equities

Public Safety and National Security. Does not reverse the long-term trend of increasing use of encrypted technologies by criminals, but could open potential avenues for cooperation with industry, without removing all law enforcement leverage (although working group participants disagree on whether calling

for legislation will provide meaningful leverage). Some working group participants, however, have indicated they think it unlikely that industry will be willing to voluntarily modify their technology - even if the threat of legislation is removed. This suggests that Option 2(a), in which the Administration would seek such technical modifications, is unlikely to succeed. However, unlike option 1, it retains flexibility on the approach should the public safety picture deteriorate to overtake competing equities. This approach would also make compromise with foreign governments not currently seeking legislation easier, but would still provide some help in resisting attempts by governments like China to use encryption policies to skew markets or oppress citizens by retaining strong public statements (e.g., "will not seek legislation").

Cybersecurity. Could encourage the use of more encryption, which would likely be good for cybersecurity. If a statement under this approach is perceived as positive but not sufficiently strong, however, this could be less successful in forestalling other nations from pursuing encryption-weakening measures. Also, because any access point to encrypted data increases risk, if government efforts to secure access are successful, this approach would reduce cybersecurity. However, the degree of impact on cybersecurity would vary significantly, and could be great or small, depending on the specific policy and technical decisions.

Economic Competitiveness. Could have a positive, though incomplete, effect in removing barriers to Administration engagement with the tech sector on this issue. Removing the prospect of United States Government calls for legislation would likely have positive effects on international competitiveness. If long-term successful in gaining government access, this option would significantly harm economic competitiveness though the harm might be somewhat mitigated if there was broad international success in getting government access.

Civil Liberties and Human Rights. Some will be dissatisfied with lack of outright disavowal, but may appreciate the pragmatic recognition of the practical limitations of a mandated approach. However, others almost certainly will continue to have concerns about government access to encrypted information being used to suppress dissident populations. Should some companies cooperate voluntarily and enable government access, the United States Government will need to accept that other

nations – including some repressive ones – will use this access as well.

Likely Reaction of Key Stakeholders

Industry and Civil Society. Although industry and civil society may be less positive to this approach than a hardline disavowal, those communities would likely see this outcome as a solid win. However, further government pressure on industry to build access into their products would likely generate negative reactions. Therefore, it is likely that Industry and Civil Society would have a much better reaction to Option 2(b), which does not seek technical modifications, thatn to Option 2(a), which does.

Other Governments. Allied governments that prefer an access regime may push back on the core U.S. message. However, those governments likely would react more positively to this approach than a complete disavowal of government access to encrypted information.

Pros

- Responds to a key ask from industry, although industry might prefer a stronger statement. To the extent that industry is satisfied with the strength of the statement, this approach could help build cooperation without limiting broader policy options.

- Could help counter the narrative that the United States is seeking to expand its surveillance capability, and help repair trust in the United States and U.S. companies overseas.

- Could allow the United States to serve as a broker between pro-access allies (e.g., United Kingdom, France, and the Netherlands), and U.S. industry, which could mitigate some demands from foreign partners and ensure U.S. companies do not have to build multiple access regimes.

- If long-term successful in gaining government access, this option would help public safety and national security.

Cons

- Could lead to disparate approaches by governments to the encryption issue, leading to more or different compliance regimes that U.S. companies will need to comply with, which

could have a negative effect on their economic competitiveness.

- Does not provide an immediate solution to the challenges that the expanding use of encryption poses to law enforcement. Without a disavowal of legislation, many U.S. technology companies in the long term likely will not pursue voluntary design changes in products and services to enable access for law enforcement.

- If long-term successful in gaining government access, this option would harm cybersecurity, economic competitiveness and civil liberties and human rights.

Option 3: Remain Undecided on Legislation or Other Compulsory Actions

Engagement Strategy and Timeline

- September: Outreach to foreign allies to assess their positions; Private outreach to key industry leaders to argue that we need a more fulsome policy discussion before we decide how to proceed.

- October: Organize or participate in closed-door, small group discussions with U.S. industry to facilitate a more in-depth policy discussion. At the same time, organize bilateral and multilateral conversations with foreign partners to discuss the challenges and how to proceed.

- November: High-level Administration statement highlights initial discussions, outlines key challenges, distills a few key questions and principals, and announces a meeting or series of meetings (potentially both domestic and international) to discuss and debate these key questions.

- December: After the discussions, reassess our position and determine whether to take a position on encryption legislation or to continue to call for discussion.

Top Line Message

- The President has said that there is no situation in which you wouldn't want strong encryption.

- At the same time, there are situations in which the government cannot obtain information related to a specific potential

national security threat. If there is not a way of accessing that information and protecting the American public, then the Administration believes need to have a public debate.

- Having a broad discussion about this is essential - over the next several months, [we or several entities] will host discussions on the challenges posed by encryption and how we can best address them. I would urge everyone to participate.

Impact on Policy Equities

Public Safety and National Security. This approach has, to date, failed to incentivize cooperation with law enforcement. It could in the long-term sway public opinion to create greater responsiveness - particularly while the government retains the leverage resulting from the threat of legislation. On the other hand, silence on our part could encourage foreign governments to control the agenda. They might pressure U.S. industry to provide lawful access, which, if successful, would make it easier for us to require similar accommodations. This approach could also encourage companies to continue to aggressively pursue developing inaccessible encrypted services, and could make future cooperation significantly more challenging. Therefore, it is hard to predict the impact that this approach would have on public safety.

Cybersecurity. Although it would not actively conflict with our message on the importance of encryption to cybersecurity, the uncertainty of public perceptions about the government's position could perpetuate distrust in encryption technologies related to the United States Government, and could undermine the effectiveness of the National Institute of Standards and Technology and other entities at a time when our cybersecurity agenda is already at risk. If long-term successful in gaining government access, this option would harm cybersecurity.

Economic Competitiveness. This approach does little to counter current distrust of the government by industry or foreign competitors. Further, by not taking a position on legislation in either direction, this approach does little to shape the reactions of other governments, increasing the risk that they will splinter into multiple camps, presenting U.S. industry with fractured markets. Therefore, this approach is likely harmful for economic competitiveness.

Civil Liberties and Human Rights. Because this approach would likely not stop - and could encourage - other nations from demanding access, it is likely harmful for the Administration's efforts on civil liberties.

Likely Reaction of Key Stakeholders

Industry/Civil Society. Will likely continue to strongly object until the United States Government explicitly eschews compulsory legislation. As time passes, if we continue to fail to take a position, industry and civil society positions will likely harden as people perceive our silence as an implicit endorsement of legislation. As a result, the United States Government risks losing credibility if it fails to participate robustly in a public debate and with a unified voice. There is also a risk that industry chooses not to participate in meetings on the subject and escalates lobbying and public relations efforts.

Other Governments. Allied governments that seek access will prefer this approach to either of the approaches that come out against compulsory legislation, and will likely see this as an opportunity for them to press for legislation themselves.

Pros

- Provides flexibility to course correct and negotiate with U.S. industry and our foreign allies.

- Retains a key negotiating chip (the threat of legislation) in our engagement with industry (although few, if any, in industry find this threat credible).

- If other governments call for legislation and/or compel companies to change their encryption solutions to enable better access in the meantime, this could provide us with cover to use that same access.

Cons

- Delays establishing a coherent Administration position, which could result in: (1) the United States being portrayed as increasingly ineffective/unable to resolve this challenge; (2) disputes among departments and agencies bleeding out into public discussion; (3) U.S. industry continuing to have challenges operating overseas (although it is unclear that a pro-encryption statement would by itself address this challenge); and (4) public and foreign government positions

may harden in the absence of an affirmative U.S. position, limiting our ability to influence the global debate.

- Does not provide an immediate solution to the challenges that the expanding use of encryption poses to law enforcement. Moreover, this approach does not resolve the current policy debate. The United States Government likely will be faced with this same discussion again in several months' time.