TECHLASH AND NATIONAL SECURITY: THE NEED FOR U.S. LEADERSHIP ON PRIVACY AND SECURITY

By Megan Brown & Dr. Andrea Little Limbago*
TECHLASH AND NATIONAL SECURITY: THE NEED FOR U.S. LEADERSHIP ON PRIVACY AND SECURITY

THIS NSI LAW AND POLICY PAPER:

1. **Summarizes** how “techlash” and criticism of Big Tech are realigning the regulatory instincts of policymakers and companies. This dynamic may embolden government action to regulate in the name of lawful government access and national security, among other goals.

2. **Describes** how movements to regulate technology companies may undermine privacy and security protective end-to-end encryption and erode Section 230 of the Communications Decency Act.

3. **Suggests** that policymakers should prioritize data protection as essential for national security in the digital era and urges U.S. global leadership to inspire digital democracies and counter digital authoritarianism.

4. **Proposes** actionable recommendations for policymakers to address encryption, federal data protection regulation, cybersecurity expertise, and global leadership.
EXECUTIVE SUMMARY
BACKGROUND
KEY ISSUES AT STAKE
AUTHOR’S VIEWS
ACTIONABLE RECOMMENDATIONS
ENDNOTES
Background

TECHLASH AS POLITICAL FORCE

- **Defining Techlash.** Techlash has been defined as the “strong and widespread negative reaction to the growing power and influence that large technology companies hold.” Techlash is the confluence of populist instincts and pro-regulation forces, which come together to target Big Tech.

- **Techlash Upends Traditional Regulatory Instincts.** Techlash is shifting policy and political alliances. Former skeptics of regulation are calling for new laws, and some in government have seized the high ground on privacy and law enforcement access.
  - Tech Has Begun to Question Self-Regulation. Some tech leaders now take the position that self-regulation is ineffective, due to fear of Techlash and a desire to preserve existing business models.

TECHLASH EMBOLDENS GOVERNMENT TO REGULATE

- **Growing Push for Regulation.** A lack of trust in Big Tech and a desire for the government to regulate may lead to new and counterproductive mandates that balkanize the use of data and overregulate.

- **Techlash Emboldens a Push for Expanded Law Enforcement Access.** Concerned about “end-to-end encryption” and platforms that cannot be compelled by law to provide access to communications, the Department of Justice (DOJ) has been working to expand law enforcement access rights and functionally limit encryption.

- **Techlash has Reignited Global “Crypto Wars.”** Governments around the world are examining encryption and lawful access to private data, with possible restrictions and bans on end-to-end encryption.
Key Issues At Stake

- **National Security Implications.** Will the push for law enforcement to have expanded government-mandated access to data weaken the United States against the range of malicious actors or will it strengthen national security due to insights gained from access to otherwise inaccessible data?

- **U.S. Global Leadership.** Will the U.S. take the global lead by formulating a modern, innovative digital policy and model for digital democracies, or will digital policies developed by authoritarian states in favor of greater surveillance proliferate?

- **The Collision Of Surveillance And Data Protection.** Will data protection regulations percolate across the U.S. that encourage the use of encryption, or will Techlash usher in weakened data protections by undermining encryption?

- **Disrupting Terrorism and Criminal Exploitation and Abuse Sites.** Will efforts like the EARN IT Act expand mandatory data access and impose operational tradeoffs for providers in a way that disrupts the tech sector, or will the status quo persist?

- **From Going Dark to a Complete Blackout.** Will the government continue to benefit from the substantial amounts of data available from American tech companies, or will data move overseas as criminals and adversaries move to non-American encrypted devices and services that do not need to comply with U.S. access requests?

Author’s Views

- **DATA PROTECTION IS ESSENTIAL FOR NATIONAL SECURITY**
  - Policymakers should prioritize data protection.
  - The United States should implement a federal digital policy focused on strengthening U.S. national security.
  - Policymakers should prioritize top down and bottom up harmonization are required in the areas of privacy and technology regulation.
To inspire digital democracies and counter digital authoritarianism, the U.S. must prevent Techno-dictators from setting global digital norms and standards.

- Europe is currently playing the role of global digital police.
- Retrenchment is not the answer.
- International institutions should be leveraged to evangelize digital democratic values.

**Actionable Recommendations**

**Obtain a Meaningful Assessment of the Ramifications of Weakening Encryption**
- Legislators should not permit Techlash and Section 230 amendments to effectively mandate encryption “backdoors.”
- Congress should designate the Government Accountability Office (GAO) or another neutral source to assess the national security and economic ramifications of encryption access policies and methods that could limit any potential negative outcomes of such policies.

**Prioritize Federal Data Protection Regulation**
- Working with industry experts, Congress should enact a federal data protection law that reinforces encryption and supports innovative uses of data for security purposes, including cybersecurity efforts.

**Deepen Cyber Expertise**
- Government must augment the cyber expertise across all levels of Law Enforcement to enhance forensics and other forms of digital tradecraft.

**Lead and Synchronize with Like-Minded Nations**
- Provide a non “command and control” counterforce to China Standards 2035.
- Promote private sector participation in global standards work.
- Partner with other liberal democracies to promote responsible and privacy-protective law enforcement and surveillance technologies.
- Invest in technology and companies that support the legitimate law enforcement and national security needs of liberal democracies.
TECHLASH UNDERMINES TRUST IN INNOVATORS

- **Defining Techlash.** Techlash has been defined as the “strong and widespread negative reaction to the growing power and influence that large technology companies hold.” It represents the confluence of populist instincts and pro-regulation forces, which come together to target Big Tech.
  
  - Recent targets of the Techlash include Facebook following scrutiny of its practices with respect to third party sharing, Google, Facebook, and Twitter for alleged political bias, social media for allegedly embracing a “culture of addiction,” and scrutiny of several tech giants under the rubric of antitrust for having too much data and power.

- **The Scope of Techlash.** Most criticisms focus on multinational tech companies, overlooking tech innovators and smaller organizations, who may be affected by regulatory policy targeted at Big Tech.

TECHLASH UPEPENDS TRADITIONAL REGULATORY INSTINCTS

- **Shifting Alliances.** Traditionally, politicians and policymakers had relatively settled approaches to regulatory philosophy and the role of government. Techlash has led some former skeptics of regulation to call for new laws, and it has allowed some in government to seize the high ground on issues like privacy and law enforcement access.

- **Industry Introspection.** For years, tech leaders were agnostic about the impact of their products and services on societal interests, such as election outcomes, political instability, and national security.
  
  - Some tech leaders themselves now take the position that self-regulation is ineffective. Some of this is driven by fear of Techlash, and a desire to preserve existing business models, while some want to get ahead of—and shape—regulation that will benefit incumbents and disadvantage competitors.
Public Opinion is Changing. Public opinion is fluid, but some surveys show a lack of trust in Big Tech and a desire for the government to regulate. Various surveys show “deep pessimism” across the political spectrum in Americans who “believe tech companies have too much power” and who are concerned about the spread of misinformation, election interference, “fake news,” and data privacy.8

- COVID-19 has elevated the public demands for security and privacy after “Zoombombing” incidents, news of some encryption keys and data stored in China, and claims about possibly misleading statements about end-to-end encryption security.9

A Global Grassroots Movement. A growing movement demanding privacy regulation has arisen across the globe.

- The European Union passed the General Data Protection (GDPR) in 2018, aimed at empowering individuals with control over data about them.
  - The GDPR requires corporations to implement certain security measures. In the first year of implementation, many of the fines issued to corporations for failing to implement these measures highlight a lack of encryption as a key problem.10
  - Key experts have noted issues in GDPR and its interpretation that could significantly challenge cybersecurity efforts.11
- Since the passage of GDPR, countries such as Japan and Brazil have pursued similar policies.12
- The California Consumer Protection Act (CCPA) represents the first major U.S. legislation to mandate broad data protection.
  - Some major U.S. companies have joined the call for comprehensive federal privacy legislation, in part to avoid concerns about individual regulation by 50 individual states, subject to a few open issues around the role of states and enforcement tools.
Relitigating Encryption. A decades old debate has resurfaced as the DOJ seeks to expand access to communications to effectuate court-ordered warrants. Concerned about “end-to-end encryption” and platforms that cannot be compelled by law to provide access to communications, the DOJ has been working to expand law enforcement access rights and functionally limit encryption.

- In the mid-1990s, the U.S. government attempted to mandate law enforcement access into software through the Clipper Chip, which was created to secure communications while also granting government access to decryption keys upon legal authorization. The discovery of a vulnerability in the Clipper Chip, coupled with backlash from privacy advocates, led to its demise. Since then, federal legislation, like the Communications Assistance for Law Enforcement Act, has excepted encryption from the scope of required law enforcement.

- The push to expand government-mandated access to data continues to resurface, with terrorist attacks in San Bernardino and Pensacola fueling calls by some for more government data access. This, despite the concerns of many Americans about the scope and nature of government surveillance.

- Facebook’s announcement of plans for end-to-end encryption and Apple’s locking down of iOS devices concerned the government and provided additional reasons to renew its focus on government-mandated access to data.

New Legislation impacting the Debate. Recent draft legislation promotes law enforcement access and has put encryption back in the spotlight. Some have argued that the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (“EARN IT Act”) would effectively “force the tech companies to break their encryption schemes.”

- While it does not explicitly reference encryption, the EARN IT Act conditions certain online liability protections on tech companies’ use of “best practices” created by a government commission to “respond to the online sexual exploitation of children ... and the proliferation of online child sexual abuse material.”

- Some security experts argue that the legislation is “a backdoor way to allow the government to ban encryption on commercial services.”

- Senators dispute the claim that the EARN IT Act could be used to weaken encryption, but do not shield encryption within the legislation.

- There are also policy voices who laud recent process changes to the law, and who think the security community is too reflexively pro-encryption, such as former government officials who have lamented the lack of progress on solutions and suggest there may be compromises that preserve law enforcement access while maintaining strong encryption.

- The legislation reflects some policymakers’ dissatisfaction with the tech community’s insistence that a safe “backdoor” is impossible. Senator Lindsey Graham (R-SC), for example, summed up this sentiment saying: “You’re going to find a way to do this or we’re going to do this for you.”
TECHLASH HAS REIGNITED GLOBAL “CRYPTO WARS”

“Crypto War” in a Digital World. Unlike the crypto wars of decades past, the current battle is happening amidst a highly digitized, connected, and global economy. What the U.S. decides in the near future will have a broad impact on security and privacy policies adopted by countries around the world. This is as it should be, because the United States has always been a leader on civil liberties, internet freedom, and digital innovation.

- In 2018, the Five Eyes issued the Joint Statement of Principles on Access to Evidence and Encryption. The statement warns that if the tech industry does not make it easier for governments to lawfully access the content and acquire decrypted versions, they will pursue other measures to achieve lawful access solutions.25
- In late 2018, Australia passed the Assistance and Access Bill for government-mandated ‘lawful’ access to data despite objections from the majority of the Australian tech community.26 Since then, competitiveness appears to have been hindered, with a movement of data to countries with greater data protection.27
- Governments, including Malawi, Turkey, India, and Ecuador, who cover over half the world’s population, have banned or are considering banning end-to-end encryption.28
Will the push for law enforcement to have expanded government-mandated access to data weaken the United States against the range of malicious actors or will it strengthen national security due to insights gained from access to otherwise inaccessible data?

- The actual national security and law enforcement impact of inaccessible data due to encrypted data remains contested.

- Encryption is one of the foundational and proven means to protect data. There is an ongoing debate about whether there is a way to permit lawful access to encrypted data, while avoiding exploitation by malicious actors and adversaries.

- There have been breaches of existing, CALEA-mandated or otherwise lawful surveillance capabilities, including unlawful Chinese access to Google law enforcement support databases.

- Last year the State Department issued “guidance” about the export of technology and services with “intended or unintended surveillance capabilities” noting such tech can “be misused to violate or abuse human rights, including the rights to freedom of expression, peaceful assembly, freedom of association, and the right to be free from arbitrary or unlawful interference with privacy.” It urges diligence in sales and wariness of certain countries, but little reason to think that such tech can be kept out of the hands of bad actors.

- Some argue that access to encrypted traffic exposes corporations, individuals, and the government to greater risk of data theft, illicit surveillance, and manipulation that could significantly and negatively impact national security.

- A U.S. encryption access policy could also inspire other governments, including adversaries and authoritarian regimes, to demand similar access to data, including the data of U.S. citizens.
U.S. Global Leadership

- Will the U.S. take the global lead by formulating a modern, innovative digital policy and model for digital democracies, or will digital policies developed by authoritarian states in favor of greater surveillance proliferate?
  - The U.S. has a great opportunity to provide the framework for a digital democracy that focuses on the American values of freedom, independence, and individual property rights. If done well, it could inspire others and help the U.S. regain global leadership at a time when authoritarian regimes are increasingly shaping global digital norms and standards.
  - The Senate is currently debating data privacy amid concerns about growing surveillance due to data sharing practices initiated during Covid-19 responses. As many countries across the globe expand government surveillance, the U.S. could introduce a counter-model that balances data privacy, public health, and national security.
  - There is an ongoing battle for global leadership, as China’s COVID-19 diplomacy looks to reshape the global system.\(^{33}\)

The Collision Of Surveillance And Data Protection

- Will data protection regulations percolate across the U.S. that encourage the use of encryption, or will Techlash usher in weakened data protections by undermining encryption?
  - Absent a federal data protection law, states are taking the lead on implementing a patchwork of data regulations and requirements.\(^{34}\)
  - Encryption is already a best practice or requirement in many regulatory settings, and it being promoted for the Internet of Things and new technology.\(^{35}\) As the Solarium Commission Report observed, “There is broad consensus across industry and the government on the importance of strong encryption. Advanced encryption of data in motion (i.e., as it is being transmitted) and at rest (i.e., as it is stored) should be a cornerstone of responsible data security.”\(^{36}\) Though the Commission hit a stalemate on law enforcement access, it recognized encryption’s foundational role.
  - The GDPR, CCPA, and a broad range of data protection legislation proposed at the state-level requires appropriate data protection such as encryption as part of the compliance regime. Companies cannot comply with requirements from both regulations that are at complete odds with one another.
Will the EARN IT Act expand mandatory data access and impose operational tradeoffs for providers in a way that disrupts the tech sector, or will the status quo persist?

- Several high-profile cases highlight the hurdles law enforcement encounters when attempting to access encrypted data during investigations. Law enforcement either fails to access potentially vital information or must incur significant costs to unlock the data, as was the case in San Bernardino.³⁷
- Regardless of whether access to encrypted communications is mandated, encryption exists and will remain a means for malicious actors to hide their communication from government authorities. There already are hundreds of encrypted messaging apps across the globe in both the licit and illicit markets.
- Dark Web forums already host exploitation and abuse sites and do not have Section 230 immunity, so there are already the legal tools to go after these forums.
- Any effort that could potentially weaken encryption would not impact those operating on these forums at all because they operate outside the law, and in fact would drive more malicious actors to these sites from commercial forums allowing them to thrive and connect.
- Even if these groups continue to use American technology and service providers for communications, it is possible that encryption will simply be pushed to earlier in the process, such as file encryption, and therefore may remain inaccessible to law enforcement.

From Going Dark to a Complete Blackout

Will the government continue to benefit from the substantial amounts of data available from American tech companies, or will data move overseas as criminals and adversaries move to non-American encrypted devices and services that do not need to comply with U.S. access requests?

- Law enforcement currently receives enormous amounts of metadata and data access from tech. companies. This data could be lost as bad actors move their communications to other forums, such as Weibo and WeChat which are highly unlikely to cooperate with the U.S. government.
  - The tech platforms reported incidents of exploitation and abuse sites 45 million times last year.³⁸
  - Apple provided gigabytes of data in response to the Pensacola shootings.³⁹
Policymakers should prioritize data protection in the digital age. The United States needs a uniform federal privacy law that can set expectations across the country and promote predictable rights and responsibilities.

The United States should implement a federal digital policy focused on strengthening U.S. national security. The U.S. continues to lag behind other countries in establishing a coherent, harmonizing federal approach to digital policy. Data protection, data integrity, and cybersecurity must be foundational to any federal digital policy.

Top down and bottom up harmonization are required. Absent a federal policy, states are implementing their own data protection legislation. There also are several disparate federal level policies, such as the cyber strategy and AI strategy, that should inform a comprehensive and consistent U.S. digital policy.

To inspire digital democracies and counter digital authoritarianism the US must prevent Techno-dictators from setting global digital norms and standards. From surveillance to cyber-attacks to censorship and internet blackouts, authoritarian regimes justify complete government access to data under the auspices of national security. This digital authoritarian playbook from China and Russia continues to inspire other countries seeking similar levels of information control. According to observers, “technology built for China’s political system is now being applied — and sometimes abused — by other governments. At least 18 countries currently use Chinese surveillance and monitoring systems.”

Europe is currently playing the role of global digital police. Some in Europe are attempting to lead the fight against digital authoritarians, but as the home to the current, dominant global tech platforms and the largest economy, U.S. leadership is required to shape global digital norms, standards, and policies. “[L]iberal democracies” need to “present a compelling and cost-effective alternative” to authoritarian digital governance. This includes leadership on surveillance and technology.
- **Retrenchment is not the answer.** A global leadership vacuum has been created as the U.S. has withdrawn influence across a variety of international forums. The U.S. should innovate in digital policy and provide the model of a functioning digital democracy that values a free, open, and secure internet that protects individual rights.

- **International institutions should be leveraged to evangelize digital democratic values.** Leadership and collaboration across international governmental organizations, such as the United Nations, World Trade Organization, International Monetary Fund, and World Bank, should be central to this renewed global engagement. Across these forums, the U.S. should develop and promote norms and policies that support a free, open, and secure internet. This includes synchronizing information security and data protection standards and norms within broader emerging technologies policies such as cyber norms, AI, quantum, 5G, cellular standards, and the like.
ACTIONABLE RECOMMENDATIONS

1 OBTAIN A MEANINGFUL ASSESSMENT OF THE RAMIFICATIONS OF WEAKENING ENCRYPTION

- Policymakers have a hard time discussing or regulating encryption and security because they lack data. Rhetoric and invective prevail among the law enforcement and technology community in debates over lawful access.
- The recent Cyberspace Solarium Commission could not reach a consensus on encryption and effectively punted, observing that while end-to-end encryption could “improve the systemic data security of the overall cyber ecosystem” and is a tool to fight repression, the benefits and costs in terms of loss of access are “hard to compare.”
- Legislators should not permit Techlash and Section 230 amendments to effectively mandate encryption “backdoors,” particularly in the absence of an honest assessment of potential tradeoffs. Charged Congressional hearings and DOJ press conferences are not conducive to collaboration nor is the reticence of providers and technologists to engage in a discussion of options.
- Before it acts, Congress should designate the GAO or another neutral source to conduct a full assessment of the national security and economic ramifications of encryption access policies and methods that could limit any potential negative ramifications of such policies.

2 PRIORITIZE FEDERAL DATA PROTECTION REGULATION

- Working with industry experts, Congress should enact a federal data protection law that reinforces encryption and supports innovative uses of data for security purposes, including cybersecurity efforts.
- Congress should take lessons learned and insights from state-level regulations and seek to harmonize across all 50 states.
3 DEEPEN CYBER EXPERTISE

- Policymakers should identify core gaps in cyber expertise and allocate resources accordingly to augment the cyber expertise of all levels of law enforcement to enhance digital forensics and other forms of digital tradecraft.

4 LEAD AND SYNCHRONIZE WITH LIKE-MINDED STATES

- The United States should introduce norms, policies, and standards that reinforce digital democracy. Provide a non “command and control” counterforce to China Standards 2035, including a specific emphasis on information security and data protection regulations, to ensure end-to-end security is a forethought as emerging technologies such as 5G and AI continue to develop.
- Government should promote private sector participation in global standards work to ensure representation of the best ideas alongside norms of access, openness, and technological neutrality.
- The United States should partner with other liberal democracies to promote responsible and privacy-protective law enforcement and surveillance technologies.
- The United States should invest in and contract with technology and companies that can and will support the legitimate law enforcement and national security needs of liberal democracies.
ENDNOTES

* Megan Brown is a Senior Fellow and Co-Director of Emerging Technologies and Cybersecurity at the National Security Institute at the Antonin Scalia Law School at George Mason University. Ms. Brown is currently a partner in Wiley Rein LLP's Telecom, Media & Technology and Privacy & Cybersecurity practices. She previously served in the Department of Justice as Counsel to two U.S. Attorneys General.

Dr. Andrea Little Limbago is a Senior Fellow and Co-Director of Emerging Technologies and Cybersecurity at the National Security Institute at the Antonin Scalia Law School at George Mason University. Dr. Limbago is currently the Vice President of Research and Analysis at Interos. She previously served as the Chief Social Scientist at Virtru and Endgame.

7 Mark Zuckerberg, Mark Zuckerberg: Big Tech needs more regulation, FIN.TIMES (Feb.16, 2020), https://www.ft.com/content/602ec7ec-4f18-11ea-95a0-43d18ec715f5.
10 Andrea Little Limbago, Lessons Learned from the GDPR’s First Year, VIRTRU (May 14, 2019), https://www.virtru.com/blog/gdpr-one-year/.
ARCTIC THAW MAKES FOR FLUID GEOPOLITICAL ENVIRONMENT.


