Comments on NAFTA Renegotiation (Docket No. USTR-2017-0006)

Before the United States Trade Representative

Jun. 12, 2017

Rapid7 submits these comments in response to the United States Trade Representative's (USTR) request for public comment on negotiating objectives regarding modernization of the North American Free Trade Agreement (NAFTA).[1] We commend USTR and the Administration for seeking to update the agreement to better reflect modern digital trade and technological development.

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to reduce the risk of a security breach, detect and investigate attacks, and build effective IT security programs. We combine world class engineering and deep insight into attacker techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks.

Summary

Technology, business practices, and the US economy have undergone considerable evolution since NAFTA was negotiated more than a quarter century ago. To reflect these changes, we urge USTR to prioritize digital trade issues as it renegotiates NAFTA and other trade agreements, and in particular to address three overarching objectives:

1. Preserve global free flow of information: Digital goods and services are increasingly critical to the US economy. However, regulations abroad that disrupt the free flow of information, such as by requiring that data be stored in a particular jurisdiction, impede both trade and innovation.
    a. *Recommendation:* NAFTA should include provisions that prevent forced localization of data, and that increase coordination on rules regarding cross-border data flow.
    b. *Recommendation:* NAFTA should include an express presumption that governments should minimize disruptions to the flow of commercial electronic information across borders.

[1] United States Trade Representative, Request for Comments on Negotiating Objectives Regarding Modernization of the North American Free Trade Agreement with Canada and Mexico, 82 Fed. Reg. 23699, May 23, 2017, https://www.federalregister.gov/documents/2017/05/23/2017-10603/request-for-comments-on-negotiating-objectives-regarding-modernization-of-the-north-american-free.

2. Promote international alignment of cybersecurity frameworks: Cybersecurity has become a global economic and safety concern. Thoughtful implementation of a cyber risk management framework can mitigate these risks and strengthen digital security. International alignment of cybersecurity frameworks help establish a common language and security baseline.
    a. *Recommendation:* NAFTA parties should recognize the importance of international alignment of computer security standards and processes for breach prevention, identification, and response.
    b. Recommendation: NAFTA should include provisions requiring the parties to develop a flexible, comprehensive cybersecurity risk management framework through a transparent process that incorporates input from public and private stakeholders.

3. Protect key security practices: Effective cybersecurity relies in part on the use of tools and activities, including strong encryption and independent security testing. Overbroad regulations that undermine or hinder such practices ultimately compromise security.
    a. *Recommendation:* NAFTA should include provisions forbidding Parties to condition market access for cryptography used for commercial applications on the transfer of private keys, algorithm specification, or other design details.
    b. *Recommendation:* If NAFTA includes provisions prohibiting circumvention of technological protection measures, those provisions should exempt non-infringing security testing of lawfully acquired protected works.

1. Preserve global free flow of information

By leveraging cloud computing, digital commerce offers significant opportunities to scale globally for individuals and companies of all sizes – not just large companies or tech companies, but for any transnational company that stores customer data. However, this growth depends on the free flow of information across international borders.

US companies seeking to provide global access to digital services are impeded by data localization – laws or norms compelling companies that do business within a country to store data associated with that country's citizens locally, rather than in data centers located elsewhere. Data localization erodes the analytic capabilities, standardization, and cost savings that cloud computing can provide. Segregating data collected from particular countries, maintaining servers locally in those countries, and navigating complex geography-based laws are all activities that require significant resources, increasing overhead costs without boosting product development or innovation. These costs can price smaller companies out of a country market entirely, which reduces the commercial choices for the citizens in the localizing country. The resulting fragmentation also undermines the fundamental concept of a unified and open global internet.

Rapid7 urges USTR to ensure that data localization is barred under NAFTA.[2] Specifically:

a. NAFTA should include provisions that prevent forced localization of data, and that increase coordination on rules regarding cross-border data flow.[3]

b. NAFTA should include an express presumption that governments should minimize disruptions to the flow of commercial electronic information across borders.[4]

2. Promote international alignment of cybersecurity risk management frameworks

When NAFTA was originally negotiated, cybersecurity was not the central concern that it is today. Cybersecurity is presently a global affair, and the consequences of malicious cyberattack or accidental breach are not constrained by national borders. At the same time that cyberattacks are growing in frequency and sophistication, huge populations increasingly rely on critical infrastructure, communications platforms, and devices and machines connected to digital technologies. Failure or disruption of these systems due to cyberattack can result in substantial economic damage, loss of personal privacy, and physical harm.

Flexible security standards are important for organizations seeking to protect their systems and data. International interoperability and alignment of cybersecurity practices would benefit US companies by enabling them to better assess global risks, make more informed decisions about security, hold international partners and service providers to a consistent security standard, and ultimately better protect global customers and constituents. Stronger security abroad will also help limit the spread of malware contagion to the US.

To keep pace with innovation and evolving threat landscapes, and to reflect a particular nation's priorities and risks, comprehensive cybersecurity risk management frameworks should ideally be flexible and capable of changing over time. To achieve this flexibility, we suggest a voluntary, transparent multistakeholder approach to developing a cybersecurity risk management framework, as

---

[2] Rapid7 supports the conclusions regarding data sovereignty of the US Dept. of Commerce's Digital Economy Board of Advisors. See First Report of the Digital Economy Board of Advisors, US Dept. of Commerce, Dec. 2016, pgs. 35-39, https://www.ntia.doc.gov/files/ntia/publications/deba_first_year_report_dec_2016.pdf.

[3] The Trans-Pacific Partnership draft (not ratified) would have barred data localization rules among its participating nations. See Trans-Pacific Partnership, Art. 14.13, Location of Computing Facilities, https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf (last accessed Jun. 9, 2017). The EU-U.S. Privacy Shield Framework articulates principles for data privacy, security, and government access aimed at enabling companies to exchange data across both jurisdictions while maintaining compliance with their respective laws. The APEC Cross Border Privacy Rules also look to provide a mechanism for dealing with cross border data privacy issues.

[4] See, for example, Statement on the Free Flow of Information and Trade in North America, Security and Prosperity Partnership of North America (April 2008), http://web.ita.doc.gov/ITI/itiHome.nsf/0657865ce57c168185256cdb007a1f3a/38ee8f5d754f3baa8525780200583b8b/$FILE/Statement%20on%20the%20Free%20Flow%20of%20Information.pdf. "[T]he co-chairs of the SPP Working Group on E-Commerce and ICT (the “Parties”) agree that all possible steps should be taken to ensure that electronic information flows freely in support of a growing and efficient North American market, within a framework of security and privacy protection."

exemplified by the National Institute of Standards and Technology's Cybersecurity Framework for Critical Infrastructure ("the Cybersecurity Framework").[5]

The Cybersecurity Framework compiles essential cybersecurity risk management processes and provides references to standards and guidance to aid adoption. The Cybersecurity Framework has already seen impressive adoption both among critical infrastructure and non-critical infrastructure organizations, companies, and government agencies.[6] Cyber Security Standards for the North American Electric Reliability Corporation – used in Canada, the United States, and parts of Mexico – are largely aligned with the Cybersecurity Framework.[7] We believe NAFTA should encourage and extend such domestic and international alignment of cybersecurity practices.

Rapid7 urges USTR to ensure that NAFTA encourages adoption of cybersecurity risk management principles.[8] Specifically:

a. NAFTA Parties should recognize the importance of international alignment of computer security standards and processes for breach prevention, identification, and response.[9]

b. NAFTA should include provisions requiring the Parties to develop a flexible, comprehensive cybersecurity risk management framework through a transparent process that incorporates input from public and private stakeholders.[10]

3. Protect key cybersecurity practices – encryption and security testing

[5] National Institute of Standards and Technology, Cybersecurity Framework for Critical Infrastructure, Feb. 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
[6] For example, the Trump Administration recently required all federal agencies to use the Cybersecurity Framework for cyber risk management. Executive Order 13800, Strengthening The Cybersecurity Of Federal Networks And Critical Infrastructure, May 11, 2017.
[7] See US Government Accountability Office, GAO-12-92, Critical Infrastructure Protection, Cybersecurity Guidance Is Available, But More Can Be Done To Promote Its Use, pgs. 35-39, Dec. 2011, http://www.gao.gov/assets/590/587529.pdf.
[8] Rapid7 supports the recommendations regarding the inclusion of cybersecurity risk management frameworks in NAFTA in the comments to USTR by the Coalition for Cybersecurity Policy and Law.
[9] The Trans-Pacific Partnership draft included a provision recognizing "the importance of using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties." See Trans-Pacific Partnership, Art. 14.16, Cooperation on Cybersecurity Matters, https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf (last accessed Jun. 9, 2017). Although helpful, this provision appears limited to cooperation on incident response. We suggest emphasizing alignment on proactive security standards that encompass prevention, identification, and response.
[10] The Trans-Pacific Partnership draft included a provision requiring the parties to endeavor to share information and experiences on regulations, policies, and compliance regarding security of electronic communications. See Trans-Pacific Partnership, Art. 14.15, Cooperation, https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf (last accessed Jun. 9, 2017). This is helpful, but the provision would be stronger if the goal were not just information exchange, but the development of a flexible and comprehensive security framework with an eye toward international alignment.

Reducing opportunities for attackers and identifying security vulnerabilities are core to cybersecurity. As the modern world is increasingly dependent on digital information, and as the consequences of cybersecurity failures grow more serious, regulations should avoid undermining key tools and activities upon which sound cybersecurity relies. Our comments focus on two such practices: strong encryption and security testing.

Prohibit requirements to weaken encryption

Encryption is a fundamental means of protecting data from unauthorized access or use. Critical infrastructure, commerce, government, and individual internet users already depend on strong security for communications, and this reliance on encryption will only continue to grow as more of the world is digitized. Weak transport security, unencrypted storage, and faulty authentication are common vulnerabilities Rapid7 has encountered in its research and practice. To protect against these and other cybersecurity flaws, Rapid7 believes companies and innovators should be able to use the encryption protocols that best protect their customers and fit their service model – whether that protocol is end-to-end encryption or some other system. However, because strong encryption can pose challenges to government access to data, some domestic and international policymakers have called for regulations that would forbid the use of strong encryption without providing a means of access to data, such as an encryption "backdoor."

Market access rules requiring weakened encryption would create technical barriers to trade and put products with weakened encryption at a competitive disadvantage with uncompromised products. Requirements to weaken encryption would impose significant security risks on US companies by creating diverse new attack surfaces for bad actors, including cybercriminals and unfriendly international governments.[11] The environment resulting from regulations to weaken encryption would most likely be highly complex, vulnerable to misuse, and burdensome to businesses and innovators – ultimately undermining the security of the end-users, businesses, and governments.[12]

Rapid7 urges USTR to ensure that NAFTA plays a role in protecting US companies' continued use of this crucial cybersecurity tool. Specifically:

a. NAFTA should include provisions forbidding Parties to condition market access for cryptography used for commercial applications on the transfer of private keys, algorithm specification, or other design details.[13]

[11] Abelson et al., *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory, Jul. 6, 2015, pg. 15, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf#page=17.
[12] Center for Democracy, CALEA II: Risks of Wiretap Modifications to End points, May 17, 2013, https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.
[13] The Trans-Pacific Partnership draft included substantially similar provisions. See Trans-Pacific Partnership, Annex 8-B, Sec. A, Information and Communication Technology (ICT) Products that Use Cryptography, https://ustr.gov/sites/default/files/TPP-Final-Text-Technical-Barriers-to-Trade.pdf (last accessed Jun. 9, 2017). Like the TPP draft, a NAFTA provision should clarify that a Party's government is not prevented from using the Party's legal

Allow TPM circumvention for independent security testing

The quantity, diversity, and complexity of digital goods and services will prevent many organizations from detecting all cybersecurity vulnerabilities without independent expertise or manpower. Independent security testing strengthens cybersecurity and helps protect consumers because researchers can call attention to vulnerabilities that manufacturers may have missed or ignored, which encourages manufacturers or other parties to make the appropriate fixes or mitigations to keep people safe.

Good faith security researchers access software and computers to identify and assess security vulnerabilities. To perform security testing effectively, researchers often need to circumvent technological protection measures (TPMs) – such as encryption, login requirements, region coding, user agents, etc. – controlling access to software, a copyrighted work. To preserve the integrity of the testing, researchers must have the ability to perform the testing independently – that is, without obtaining authorization to circumvent a TPM from the rightsholder of copyrighted software. However, this activity is often chilled by Sec. 1201 of the Digital Millennium Copyright Act (DMCA) of 1998, which forbids unauthorized circumvention.[14]

Good faith security researchers do not seek to infringe copyright, or to interfere with a rightsholder's normal exploitation of protected works. Rather, researchers seek to evaluate and test software for flaws that could cause harm to individuals and businesses – a broadly beneficial and non-infringing activity. The US Copyright Office recently affirmed that security research is fair use and granted this activity, through its triennial rulemaking process, a temporary exemption from the DMCA's requirement to obtain authorization from the rightsholder before circumventing a TPM to safely conduct security testing on lawfully acquired consumer products.[15] The Copyright Office's exemption was a significantly positive step for independent researchers seeking to strengthen the security of digital products and services.

Some previous trade agreements have closely mirrored the DMCA's prohibitions on unauthorized circumvention of TPMs controlling access to a copyrighted work.[16] This approach replicates internationally the overbroad restrictions on independent security testing that the US is now scaling back. Newly negotiated trade agreements should aim to strike a more modern and equitable balance between copyright protection and good faith cybersecurity research.

If a renegotiated NAFTA includes provisions forbidding the unauthorized circumvention of TPMs that rightsholders use in connection with the exercise of their rights, Rapid7 urges USTR to provide for

---

procedures to compel a service provider to produce unencrypted communications if the service provider has access to those communications.

[14] 17 USC 1201(a)(1)(A).

[15] U.S. Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R. 201, Oct. 28, 2015, pgs. 48-51, http://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf.

[16] For example, Article 18.4 of the Korea-U.S. Free Trade Agreement (KORUS FTA), signed in 2007, which reflects much of the language of 17 USC 1201.

more flexible exceptions and limitations for non-infringing security research than the language of the DMCA.[17] Specifically:

b. Any anti-circumvention provisions of NAFTA should be accompanied by provisions clarifying that the prohibition on circumventing TPMs does not apply to non-infringing security testing of lawfully acquired protected works.

* * *

We appreciate the opportunity to share our views. If there are additional questions or if Rapid7 can provide any further assistance, please contact Harley Geiger, Director of Public Policy, at Harley_Geiger[at]Rapid7.com. Thank you.

END

[17] The Trans-Pacific Partnership draft included a more flexible approach than KORUS, enabling parties to provide certain exceptions and limitations to enable non-infringing uses adversely impacted by the prohibition on circumvention. However, under TPP, these exceptions must be arrived at through a legislative, regulatory, or administrative process. See Trans-Pacific Partnership, Art. 18.68(4)(a), Technological Protection Measures, https://ustr.gov/sites/default/files/TPP-Final-Text-Intellectual-Property.pdf (last accessed Jun. 9, 2017). We suggest proactively exempting good faith independent security testing from any prohibition on circumvention.