



Comments on Competition and Consumer Protection in the 21st Century Hearings

Before the Federal Trade Commission
Docket No. FTC-2018-0052

Aug. 20, 2018

Rapid7 submits these comments in response to the Federal Trade Commission's (FTC)'s request for public input in advance of its Hearings on Competition and Consumer Protection in the 21st Century.¹

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cyber security. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and 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.

Continued support for efforts to improve data security

The FTC has long been at the forefront of federal agencies promoting strong data security practices, through education and awareness, reports, events, and enforcement activity. For example, since its 2012 Privacy Report,² the FTC has applied security principles for online and offline data to diverse technologies and business models, including the recent staff report on the Internet of Things (IoT).³ The FTC routinely holds events and seminars on key issues involving data security, such as its recent workshops on connected vehicles and ID theft,⁴ and provides resources to consumers and small businesses about basic security measures.⁵ The FTC has also identified data security as a key enforcement priority for several years.⁶

¹ FTC, *Hearings on Competition and Consumer Protection in the 21st Century*,

<https://www.ftc.gov/policy/hearings-competition-consumer-protection> (last accessed Aug. 20, 2018).

² FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*, Mar. 2012, <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers>.

³ FTC Staff Workshop Report, *The Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), available at <https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things>.

⁴ FTC, *Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles*, Jun. 28, 2017, <https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected>. FTC, *Identity Theft: Planning for the Future*, May 24, 2017, <https://www.ftc.gov/news-events/events-calendar/2017/05/planning-future-conference-about-identity-theft>.

⁵ FTC, *Engage, Connect, Protect, Staff Perspective*, Apr. 2018, https://www.ftc.gov/system/files/documents/reports/engage-connect-protect-ftcs-projects-plans-foster-small-business-cybersecurity-federal-trade/ecp_staffperspective_2.pdf.

⁶ Prepared statement of the Federal Trade Commission, before the Senate Committee on Appropriations, Subcommittee on Financial Services and General Government, Review of the FY2019 Budget Request for the

Rapid7 commends the Commission's appropriately strong focus on data security. Data security is increasingly important to consumer protection and success of businesses of all sizes. We expect this trend to accelerate, in particular as IoT continues to bridge divides between

Rapid7 urges the FTC to continue its support for awareness efforts, thought leadership, and enforcement priorities around the issue of data security.

Effective and consistent data security requirements

The FTC has indicated that it "stands ready, willing and able to work with Congress" on the issue of comprehensive data security legislation.⁷ The FTC has also set a goal of "working with other agencies to use its complementary authority to protect consumers as effectively and efficiently as possible, to avoid duplication, and to promote consistency."⁸ Data security continues to deserve FTC's close attention to develop solutions that protect consumers, provide clear and consistent standards, and are flexible enough to be practicable for a wide range of entities.

Rapid7 supports streamlined and holistic security requirements for personal information that preempt similar state laws. Disparate data security and breach notification laws do not serve consumers or businesses well. Consumers in different jurisdictions are subject to uneven levels of protection, and the sheer complexity of the laws makes it more difficult for businesses of all sizes to comply. At least 17 states require minimum security standards for personal information held by the private sector, all 50 US states (and the District of Columbia) have data breach notification laws, and international laws such as GDPR add new security requirements on data processing.⁹ At the same time, data breaches and security incidents continue to grow in frequency despite existing laws and class action lawsuits.

Provisions addressing security requirements should be included in efforts to establish federal privacy or breach notification laws. Notification requirements and common law causes of action only apply after a breach has occurred. Data security safeguards are critical to reducing the risk of breaches before they occur. Security is also a key component of privacy protection frameworks. While privacy is not achieved through security alone, data security is critical to protect against risks to collected data that arise from unauthorized system use or behavior – such as malicious hacking and accidental data exposure – that can lead to privacy infringement.

Rapid7 believes a national data security requirement should preserve flexibility through a risk

FCC and the FTC, May 17, 2018, pg. 10, <https://www.appropriations.senate.gov/imo/media/doc/051618%20-%20FTC%20Simons%20Testimony1.pdf>.

⁷ *Id.*, pg. 7.

⁸ Prepared Statement of the Federal Trade Commission, before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law, Examining the Proposed FCC Privacy Rules, May 11, 2016, pg. 2, <https://www.ftc.gov/public-statements/2016/05/prepared-statement-federal-trade-commission-examining-proposed-fcc-privacy>.

⁹ National Conference of State Legislatures, Data Security Laws, State Government, Dec. 5, 2017, <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>.

management approach. This approach could require reasonable technical, physical, and administrative safeguards to control risks to personal information that the organization identifies through a risk assessment. Reasonableness should be assessed in light of the nature of the organization and the sensitivity of information it maintains, and the regulation should not be overly prescriptive regarding what components must be in a security plan. A benefit of this approach is that not all data would need to receive the same level of protection, and the same expectation is not necessarily held for a small business as for a large global enterprise. Organizations could apply strict safeguards to especially sensitive data, and more basic measures for less sensitive data – in proportion to the risks – but some protection would be in place for all data covered by the law. This approach can help security requirements remain effective over time for a variety of organizations without undue burden.

Rapid7 supports data security requirements that are not limited solely to protecting against economic or physical harm. Limiting safeguards to protection against economic harm would not align with user expectations or the wide array of threats organizations face today, and would be a step back from existing protections in many states. Numerous states require the private sector to safeguard personal information without limiting these safeguards to protection against risks of economic harm.¹⁰ Several states require protecting credentials for online accounts without limiting protection to credentials necessary for financial transactions.¹¹ Modernized cybersecurity standards should reflect that sensitive non-financial information warrants some baseline of reasonable protection against unauthorized access. However, the flexible approach we support – outlined above – may apply more stringent security measures for information that can directly lead to economic harm, and less for other types of personal information.

Many state laws and federal legislative proposals define personal or covered information as always requiring an individual's actual name – first and last name or first initial and last name. Under these definitions, data security requirements would not apply to usernames/passwords, ID numbers, personal media, biometrics, or medical information (not covered by HIPAA/HITECH), unless the user's actual name were also included. We believe this name requirement is anachronistic and should be dropped or limited. Frequent redistribution and aggregation of breached data has made it easier to combine data elements from multiple breaches and open sources.¹² A breached username/password, biometric authenticator, or in some cases photographic images – with the growing sophistication and availability of biometric recognition and search – can yield a user's actual name.

¹⁰ Alabama S.B. 318, Act No. 396, Sec. 3(a)-(b), 2018. Arkansas Code Ann. 4-110-104. California Civ. Code 1798.81.5(b). Connecticut Gen. Stat. Sec. 42-471(a). Florida Stat. 501.171(2). Indiana Code 24-4.9-3-3.5. Kansas Stat. 50-6,139b(b)(1). Massachusetts Gen. Laws Ch. 93H Sec. 2(a). Minnesota Stat. 325M.05. New Mexico Stat. 57-12C-4. Nevada Rev. Stat. 603A.210, Oregon Rev. Stat 646A.622(1). Rhode Island Gen. Laws 11-49.3-2. Texas Bus. & Com. Code 521.052. Utah Code 13-44-201.

¹¹ Alabama S.B. 318, Act No. 396, Sec. 2(6)(a)(6), 2018. California Civ. Code 1798.81.5(d)(1). Florida Stat. 501.171(1)(g)(b). Maryland Code Com. Law 14-3501(e). Minnesota Stat. 325M.01. Nevada Rev. Stat. 603A.040.

¹² See Statement of Troy Hunt for the House Committee on Energy and Commerce, Identity Verification in a Post-Breach World, pgs. 9-11, Nov. 30, 2017, <http://docs.house.gov/meetings/IF/IF02/20171130/106662/HHRG-115-IF02-Wstate-HuntT-20171130.pdf>. Frequent redistribution and aggregation of breached data has made it easier to combine data elements from multiple breaches and open sources.

We urge the Commission to continue to actively lend its experience and knowledge in discussions about preemptive federal security requirements. We hope the security community has the opportunity to collaborate with the FTC to develop modernized, streamlined, and effective data security standards and guidance.

Good faith security research

Independent security researchers access software and computers to identify and assess security vulnerabilities. This may refer to users or administrators who uncover issues incidentally or accidentally, or security professionals who intentionally test systems to identify problems, and raise awareness to vendors and users so the issue is resolved. This research strengthens cybersecurity and helps protect consumers because the researchers 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. Yet well-intentioned regulatory proposals to protect consumer privacy and security can chill standard security research practices by broadly restricting independent access to data.

The FTC has previously expressed support for "white hat" security researchers in Congressional testimony and through FTC-hosted events such as PrivacyCon.¹³ The FTC has recommended that companies should communicate and coordinate with the security research community as part of a continuous process of detecting and remediating software vulnerabilities.¹⁴ The FTC has noted that, though deterring criminal behavior and malicious hacking is an important goal, overbroad restrictions on access to software and systems for cybersecurity research purposes would be detrimental to consumers' privacy, security, and safety.¹⁵

Rapid7 commends the FTC's forward-looking posture on good faith security research. We urge the Commission to continue working with federal and state agencies and legislatures to ensure new regulations on access and use to computers and software do not unduly restrict independent research of cybersecurity vulnerabilities.¹⁶

¹³ FTC, PrivacyCon 2017, Jan. 12, 2017, <https://www.ftc.gov/news-events/events-calendar/2017/01/privacycon>.

¹⁴ FTC Public Comment on NTIA Safety Working Group's "Coordinated Vulnerability Disclosure 'Early Stage' Template", Feb. 15, 2017, pgs. 1-2, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-national-telecommunications-information-administration-regarding-safety-working/170215ntiacomment.pdf.

¹⁵ Prepared statement of the Federal Trade Commission, before the House Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, Examining Ways to Improve Vehicle and Roadway Safety, pgs. 5-6, <https://docs.house.gov/meetings/IF/IF17/20151021/104070/HHRG-114-IF17-Wstate-MithalM-20151021.pdf>.

¹⁶ Questions for the Record for Maneesha Mithal, before the House Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, Examining Ways to Improve Vehicle and Roadway Safety, pg. 2, Oct. 21, 2015, <https://docs.house.gov/meetings/IF/IF17/20151021/104070/HHRG-114-IF17-Wstate-MithalM-20151021-SD005.pdf>.

Vulnerability disclosure and handling processes

Rapid7 urges the Commission to continue its support for coordinated vulnerability disclosure and handling processes through education efforts (such as policy reports and guidance) and enforcement activities (such as consent decrees). In addition, Rapid7 urges the FTC to adopt an agency-wide process for receiving, analyzing, and appropriately mitigating vulnerabilities relating to FTC systems and resources from external or internal sources, as advised by the NIST Cybersecurity Framework.¹⁷

The FTC has recommended that "companies that provide Internet-connected products or collect sensitive consumer information should consider implementing a vulnerability disclosure policy and related processes."¹⁸ The FTC has advised organizations to adopt vulnerability disclosure and handling processes in data security guidance and policy reports.¹⁹ Several FTC consent orders also required data security programs that included review, assessment, and response to third party vulnerability reports.²⁰

Recognizing that there is no perfect security and that all vulnerabilities cannot be completely eliminated from digital goods and services pre-market, organizations must be prepared to continually identify and respond to cybersecurity flaws in their infrastructure and networks throughout the product lifecycle. Yet the quantity, diversity, and complexity of vulnerabilities will prevent many organizations from detecting all vulnerabilities without independent expertise or manpower. This may be especially true for organizations with limited experience or resources for cybersecurity.

It is increasingly crucial to foster an environment where vendors take disclosure of security issues from external sources – such as independent security researchers – seriously and openly, rather than with legal threats or avoidance. To do this effectively, it is critical for organizations to have a plan and policy in place to receive and process vulnerability information from external sources, such as independent security researchers. Businesses and government agencies are increasingly implementing vulnerability disclosure and handling processes, but adoption of flexible and mature processes for handling unsolicited vulnerability reports is not yet the norm.

Vulnerability disclosure and handling processes are formal internal mechanisms for receiving, assessing, and mitigating security vulnerabilities submitted by external sources, such as

¹⁷ National Institute of Standards and Technology, Cybersecurity Framework Version 1.1, RS.AN-5, Apr., 16 2018, pg. 42, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

¹⁸ FTC Public Comment on NTIA Safety Working Group's "Coordinated Vulnerability Disclosure 'Early Stage' Template", Feb. 15, 2017, pg. 5, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-national-telecommunications-information-administration-regarding-safety-working/170215ntiacomment.pdf.

¹⁹ See, for example, FTC, Start with Security: A Guide for Business, Jun. 2015, pg. 12, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

²⁰ See, for example, FTC, Proposed Consent Agreement, Uber Technologies, Inc., 83 Fed. Reg. 18064, Apr. 25, 2018, <https://www.gpo.gov/fdsys/pkg/FR-2018-04-25/pdf/2018-08600.pdf>. See also FTC, In the Matter of ASUSTeK Computer Inc., Decision and Order, Docket No. C-4587, Jul. 18, 2016, pg. 4, <https://www.ftc.gov/system/files/documents/cases/1607asustekdo.pdf>.

independent researchers acting in good faith, and communicating the outcome to the vulnerability reporter and affected parties.²¹ Such processes do not apply to a vendor's products and services alone. Organizations should be prepared to receive disclosures regarding vulnerabilities in their infrastructure and system configuration as well. If an organization receives a vulnerability that actually applies to another vendor's products, the organization should nonetheless have a process for receiving the vulnerability and passing it on to the appropriate vendor.

Establishing a coordinated vulnerability disclosure and handling process – and communicating the existence and scope of that policy publicly – can help organizations quickly detect and respond to vulnerabilities disclosed to them by external sources, leading to mitigations that enhance the security, data privacy, and safety of their systems. Vulnerability disclosure and handling processes can also help protect researchers or accidental discoverers acting in good faith by providing them with a clear channel to communicate vulnerabilities to technology providers and operators, reducing the risk of conflict or misunderstanding. Such processes may or may not actually incentivize searching for vulnerabilities (such as by offering bounties for bug submissions), or provide a guarantee of legal liability protection.

Rapid7 believes processes for receiving, reviewing, and responding to vulnerability disclosures should be considered a basic, and relatively easily achievable, component of modern cybersecurity plans. As we increasingly depend on complex and flawed software and systems, we must pave the way for greater community participation in security. Facilitating communication between technology providers and vulnerability discoverers is an important step toward greater collaboration aimed at keeping consumers safe.

*

*

*

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](mailto:Harley_Geiger[at]Rapid7.com). Thank you.

END

²¹ Note, such processes are not necessarily "bug bounty programs" and may not offer incentives to vulnerability reporters. Bug bounty programs are a subset of coordinated vulnerability disclosure and handling processes. Organizations will need to determine for themselves whether offering incentives for disclosures is the best fit for them.