Addressing Privacy and Security Concerns with Distributed Tech without Impeding Innovation

Working Paper

By Krisztina Pusok[1]

[1] American Consumer Institute Center for Citizen Research

Introduction

In May 2018, the Federal Bureau of Investigation (FBI) published a warning notifying that Russian computer hackers had compromised hundreds of thousands of home and office routers and could collect user information or shut down network traffic.[2] The Bureau then urged the owners of several brands of routers to turn them off and on again, and to download firmware updates from the manufacturers. While the FBI warning highlighted the potential danger of routers built on open source code, the warning may have gone largely unnoticed by most consumers.

Software and firmware has become ubiquitous in our daily lives, directing Internet of Things (IoT) devices and applications that are key to modern commerce, urban planning and management, logistics, agriculture, and to critical infrastructure, just to name a few areas. Yet, despite the promising and necessary growth in IoT devices and applications, cyberattacks, data breaches, and data misuse scandals are on the rise,[3] having more far-reaching consequences and becoming a real danger for both brands and customers.

To make matters even worse, the use of open source everywhere as a cost-effective way to allow customization has the potential to exacerbate privacy and cybersecurity problems in the IoT ecosystem. This paper seeks to address the opportunities and challenges presented by the use of open source and provide a discussion of the risks associated with the use of open source in IoT devices.

---

[2] Joseph Menn and Sarah N. Lynch, "FBI Warns Russians Hacked Hundreds of Thousands of Routers," Reuters, May 25, 2018, https://ca.news.yahoo.com/fbi-says-foreign-hackers-compromised-home-router-devices-155414530.html.

[3] Dennis Green, "If You Shopped at These 15 Stores in the Last Year, Your Data Might Have Been Stolen," Business Insider, July 1, 2018, https://read.bi/2q2ryJ0 .

The issue of data privacy and cybersecurity is increasingly captured by multiple regulatory frameworks, creating a complex regulatory environment. In addition to exploring the potential risks these technologies may present to consumers, this paper also discusses the regulatory alternatives (top-down regulations versus voluntary alternatives) in dealing with the privacy and security concerns posed by open source in the IoT space. The paper concludes by outlining policy solutions that aim to protect consumers without impeding innovation.

Privacy and Cybersecurity Risks with IoTs

Internet of Things (IoT) devices are largely known as computing devices that are connected to a network that is publicly accessible. Such devices, ranging from home routers and security cameras to baby monitors, thermostats, and cars, are connected to the internet, multiplying the number of potential threat vectors for data breaches and further complicating the IoT privacy and security environment. As such, securing IoT devices is a collective action problem in that the actions and cooperation of many stakeholders are required to address the changing landscape.[4]

Worldwide, the number of IoT devices aside from smartphones, tablets, and laptops recently outstripped the number of mobile phones.[5] In addition, the IoT market is

[4] Anne Hobson. "The Resilience Approach to Cybersecurity Policy in the Internet of Things Ecosystem." July 2019, Policy Paper 2019.004, Center for Growth and Opportunity.
[5] Knud Lasse Lueth, "State of the IoT 2018: Number of IoT Devices Now at 7B—Market Accelerating," IoT Analytics, August 8, 2018, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

expected to more than double, to $520 billion, between 2017 and 2021, with data centers and analytics as the fastest-growing subsectors.[6]

The interconnected and complex nature of the IoT ecosystem raises major security and privacy concerns.

Security vulnerabilities in these devices not only can lead to major privacy breaches, but can also have severe economic and safety implications. With respect to privacy[7], sensor nodes in devices, like wearables as well as personal assistance and smart home appliances, have the capability to capture highly personal data that be breached or misused. As the complexity of the IoT ecosystem continues to grow with more and more devices getting connected, the number of attack vectors and possibilities for hackers will grow rapidly.

A defining characteristic of IoT devices is the pervasive and often nontransparent collection and seamless linkage of user data to provide personalised experiences. Such characteristics, however, can create numerous privacy cybersecurity risks, which are frequently designed to go unnoticed by users in order to provide a more seamless experience.[8]

---

[6] Ann Bosche et al., “Unlocking Opportunities in the Internet of Things,” Bain & Company, August 7, 2018, https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/

[7] A. Weber, S. Reith, D. Kuhlmann, M. Kasper, J. Seifert and C. Krauß, "Open Source Value Chains for Addressing Security Issues Efficiently," 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, 2018, pp. 599-606.

[8] Scott R Peppet, “Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent” (2014) 93 Texas Law Review 85.

Among the more obvious specific threats is that many manufacturers and vendors of IoT devices do not have the know-how of how to technically address security issues, with many of them being unaware that such problems even exist.[9] Another primary common concern[10] is the lack of transparency with the end consumer concerning the types of data controls and ownership responsibilities that need to be in place to ensure a secure environment. For example, research by the Center for Democracy and Technology finds that cyber insecurity is due to information asymmetry between buyers and sellers of IoT devices, or malware-related disruptions not necessarily borne by the owners of the devices, and moral hazard in that consumers bear the costs of the risky actions of device manufacturers.[11]

As IoT systems bear great potential in areas such as health and wellness, utilities, urban planning and management, logistics, and supply chain management, agriculture, and commerce, concerns around privacy and data protection require serious consideration.

Open source software and hardware paths for IoT devices require especially serious consideration for reasons discussed below.

[9] Mansfield-Devine, Steve. "Open source and the Internet of Things." Network Security 2018, no. 2 (2018): 14-19.
[10] Ibid.
[11] Benjamin C. Dean, “An Exploration of Strict Products Liability and the Internet of Things,” Center for Democracy & Technology, 2018.

The Role of Open Source

Open source code has grown in popularity over the years and is used by companies of all sizes, across all industries. According to a 2017 Forrester Research report, open source code's preeminence in application development, with proprietary custom code comprising only 10% to 20% of applications.[12]

Open source has become an essential element in application development today, as it saves developers time and it saves companies and consumers money.

From a security standpoint, open source is neither more nor less secure than custom code. Yet, there are certain characteristics[13] with open source code that make its vulnerabilities particularly attractive to attackers: it is widely used in commercial software and hardware applications; it leverages a "pull" support model[14] that places more responsibility on the consumers to track vulnerabilities, as well as fixing and updating the software of firmware; known vulnerabilities are publicly published on the Common Vulnerabilities and Exposures (CVE) database[15], providing a roadmap for exploiting code. These key characteristics provide hackers a target-rich environment.

---

[12] Amy DeMartine, "The Forrester Wave: Software Composition Analysis, Q1 2017," Forrester Research, February 23, 2017, www.blackducksoftware.com/sites/default/files/images/Downloads/Reports/USA/ForresterWave-Rpt.pdf.
[13] "2017 Open Source Security and Risk Analysis," BlackDuck, https://www.blackducksoftware.com/open-source-security-risk-analysis-2017.
[14] "2018 Open Source Security and Risk Analysis Report," BlackDuck by Synopsys Center for Open Source Research & Innovation, 2018, https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/2018-ossra.pdf.
[15] The U.S. government funds and the MITRE Corporation operates a public database of software vulnerabilities (see www.cve.mitre.org). Each listed vulnerability is assigned a unique CVE identifier that contains information about a specific vulnerability's capacities and risks.

Empirical evidence from a recent analysis[16] conducted by the American Consumer Institute shows that that 5 of every 6 Wifi routers are inadequately updated for known security flaws,[17] leaving connected devices open to cyberattacks that can compromise consumer privacy and lead to financial loss. The suggest that the most popular consumer Wi-Fi routers are inadequately updated for security, leaving IoT devices open to malicious attacks with potentially disastrous results. The results also suggest that Wi-Fi router manufacturers are neglecting to update their firmware for known vulnerabilities and that the problem is likely more pervasive for other IoT devices.

Besides risks associated with firmware vulnerabilities, IoT devices are also at high risk for open source software vulnerabilities, as hackers depend on Trojan viruses, malicious scripts, and malware to disable IoT systems.[18]

Another study published by the American Consumer Institute shows the prevalence of open source vulnerabilities in software applications.[19] The results show an average of 6

---

[16] Krisztina Pusok. "Securing IoT Devices: How Safe Is Your Wi-Fi Router?", American Consumer Institute Center for Citizen Research, 2018, www.theamericanconsumer.org/wp-content/uploads/2018/09/FINAL-Wi-Fi-Router-Vulnerabilities.pdf .

[17] Out of the 186 sampled routers, 155 (83%) were found to have vulnerabilities to potential cyberattacks in the router firmware, with an average of 172 vulnerabilities per router, or 186 vulnerabilities per router for the identified 155 routers. In total, 32,003 known vulnerabilities found in the sample. For more details about the analysis see Krisztina Pusok. "Securing IoT Devices: How Safe Is Your Wi-Fi Router?" 2018.

[18] Matthews, K. "The Current State of IoT Cybersecurity." Available online: https://www.iotforall.com/current-state-iot-cybersecurity/.

[19] Krisztina Pusok. "HOW SAFE ARE POPULAR APPS? A Study of Critical Vulnerabilities and Why Consumers Should Care," American Consumer Institute Center for Citizen Research, 2018, www.theamericanconsumer.org/wp-content/uploads/2018/12/8.5x11_VZ_American-Consumer-Institute_Popular-Apps_D2.pdf

vulnerabilities per application over the entire sample,[20] while 43% among the detected vulnerabilities are considered critical or high risk by the National Vulnerability Database.

Issues related to open source vulnerabilities in both software and firmware remain largely unnoticed by the general public. Yet, these issues are pervasive and could be present in most consumer devices. The evidence presented here is corroborated by previous studies and underlines the need for more governance to prevent serious attacks and privacy breach.

IoT Governance: Challenges

Between 2005 and 2016, the annual number of software open source vulnerabilities reported by the CVE database fluctuated between 5,000 and 8,000. In 2017, the number of reported exploits, had already reached 15,000.[21] As software and firmware using open source components are increasingly being used in critical infrastructures including food supply, in traffic systems, and with industrial robots, flaws or attacks can also have negative effects on consumer safety.

Evidence indicates that the first wave of attacks targeting IoTs started in 2016, when the hackers mainly targeted routers and IP cameras.[22] Symantec's annual Internet Security

[20] The study scrutinizes 330 of the most popular Android apps in the U.S., drawn from 33 different categories. Of the sample, 105 apps (32% of the total) were identified to contain vulnerabilities across a number of severity levels – critical, high, medium and low risk – totaling 1,978 vulnerabilities.
[21] A. Weber, S. Reith, D. Kuhlmann, M. Kasper, J. Seifert and C. Krauß, "Open Source Value Chains for Addressing Security Issues Efficiently," 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, 2018, pp. 599-606.
[22] Matthews, K. The Current State of IoT Cybersecurity. Available online: https://www.iotforall.com/current-state-iot-cybersecurity/

Threat Report found a 600% increase in IoT attacks in 2017.[23] Not only the number of IoT attacks is expected to increase, but also the economic costs associated with the attacks. The annual cost of cybercrime damage to consumers, companies and governments is expected to reach $2 trillion by the end of 2019 – up from $500 billion in 2016.[24]

The privacy and security requirements we want for our devices and software is rather simple. We want these devices to be free from intrusion, and we want the data to be secure, not corruptible and certainly not distributable without the owner's authorization. Yet, empirical evidence shows that these devices are highly vulnerable, and are becoming an increasingly attractive target for cyberattacks. Unsurprisingly, cyber and data insecurity is increasingly viewed as a market failure in need of a comprehensive legislative solution at the international, federal, and state level.

In Europe, the legal landscape recently experienced a significant change with the General Data Protection Regulation (GDPR) that came into force on May 25, 2018.

Hundreds of laws relating to privacy and data protection, including common law torts, criminal laws, evidentiary privileges, federal statues, and state laws, already exist in the US.[25] Yet, in the aftermath IoT security failures and data breaches, policymakers are pursuing formal laws and regulations to address cyber insecurity and related data

[23] "Internet Security Threat Report," Symantec, Volume 23, April 2018, https://www.symantec.com/security-center/threat-report.
[24] Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019," Forbes, January 16, 2016, www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#f4bae343a913 .
[25] Layton, Roslyn, and Julian McLendon. "The GDPR: What It Really Does and How the US Can Chart a Better Course. Fed." Soc. Rev 19 (2018): 234-248.

privacy concerns. At the state level, California passed the California Consumer Privacy Act (CCPA) of 2018 as well as a separate bill that requires “reasonable security features” for connected devices.[26]

The pace of development of privacy and data protection law is significantly faster than that of other kinds of law.[27] While both the GDPR and the CCPA seek to set a legislative precedent for how we govern data security and privacy, it is important to acknowledge the unique complexity of the governance challenge facing the IoT ecosystem. More specifically, further discussion is required around the trade-offs of a strict regulatory approach that has the potential to discourage innovation and adaptability and offset the ecosystem’s capability[28] to manage risk.

A. Top-Down Approaches

The goal of GDPR was to create a harmonised data protection standard across the European Union in order to strike a balance between the free flow of data and the fundamental interests of data subjects (e.g. privacy). As the IoT collects, processes, and shares substantial volumes and varieties of personal data, the GDPR must be treated as a key governance framework for the design and deployment of IoT systems.

---

[26] 2018 Cal. Legis. Serv. Ch. 886 (S.B. 327) (to be codified at Cal. Civ. Code § 1798.91.04). See also Gibson, Dunn & Crutcher, “New California Security of Connected Devices Law and CCPA Amendments,” October 5, 2018, https://www.gibsondunn.com/new-california-security-of-connected-devices-law-and-ccpa-amendments/

[27] Layton, Roslyn, and Julian McLendon. "The GDPR: What It Really Does and How the US Can Chart a Better Course. Fed." Soc. Rev 19 (2018): 234-248.

[28] Anne Hobson. “The Resilience Approach to Cybersecurity Policy in the Internet of Things Ecosystem.” July 2019, Policy Paper 2019.004, Center for Growth and Opportunity.

Evidence shows that a regulatory approach modeled after GDPR could result in trade-offs including fewer choices for consumers and less competition from innovators.

In the absence of a federal rule in the US, California[29] recently passed the California Consumer Privacy Act (CCPA) and the Security of Connected Devices Act with the goal to protect consumer privacy and secure IoTs. The laws, expected to go into effect in 2020, will impose new rules for IoT manufacturers and businesses collecting consumer data. It has been argued that for many businesses the impact of the laws will be limited. [30]

Empirical evidence suggests that we should be at the very least cautious of the impact these top-down regulatory approaches.

Among the documented impacts is the effect on small and medium sized businesses. For example, data suggests that small and medium sized advertising tech competitors have lost up to one-third of their market position since the GDPR took effect.[31] Other similar studies suggest that several American retailers, game companies, and service providers have completely left the European market.[32]

---

[29] Hawaii and New Mexico are also considering broad privacy legislation modeled on California's CCPA law.

[30] Grant Gross. "Potential impact of two IoT security and privacy laws on tech industry." December 19, 2018, https://www.hpe.com/us/en/insights/articles/potential-impact-of-two-iot-security-and-privacy-laws-on-tech-industry-1812.html

[31] Björn Grelf, "Study: Google Is the Biggest Beneficiary of the GDPR," Cliqz, October 10, 2018, https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr

[32] See Allison Schiff, "Drawbridge Sells Its Media Arm and Exits Ad Tech," AdExchanger, May 8, 2018, https://adexchanger.com/data-exchanges/drawbridge-sells-its-media-arm-and-exits-ad-tech/; Ronan Shields." Verve to Focus on US Growth as It Plans Closure of European Offices Ahead of GDPR," Drum, April 18, 2018, https://www.thedrum.com/news/2018/04/18/verve-focus-us-growth-it-plans-closure-european-offices-ahea

The GDPR has also proven to be threatening for innovation and research. Not only that many GDPR requirements have been found to be incompatible with big data, artificial intelligence, blockchain, and machine learning, but for many technology developers, engineers, and entrepreneurs, the regulation has created uncertainty not only in the text of the law but also in that requirements of the GDPR conflict with the operation of machine learning and artificial intelligence.[33]

From the cybersecurity perspective, evidence shows that the GDPR has increased cybersecurity risks by undermining the transparency of the international systems and architecture that organizes the internet.[34]

Further research also shows that the GDPR creates risks for identity theft and online fraud,[35] increases compliance costs for firms to the point of bankruptcy,[36] and it has contributed to the direct welfare loss affecting European consumers.[37]

---

d-gdpr ; Owen Good, "Super Monday Night Combat Will Close Down, Citing EU's New Digital Privacy Law," Polygon, April 28, 2018, https://www.polygon.com/2018/4/28/17295498/super-monday-night-combat-shutting-down-gdpr .

[33] Joel Thayer and Bijan Madhani, "Can a Machine Learn Under the GDPR?," TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy, December 16, 2018, https://ssrn.com/abstract=3141854

[34] Roslyn Layton, "Trump Should Ignore Chinese Manufacturers' Phony Promises," Forbes, February 20, 2019, https://www.forbes.com/sites/roslynlayton/2019/02/20/trump-should-ignore-chinese-manufacturers-phony-promises/#257b924d50ec

[35] Roslyn Layton, "The 10 Problems of the GDPR," AEI, March 12, 2019, http://www.aei.org/press/aei-tech-regulation-expert-roslyn-layton-testifies-on-europes-general-data-protection-regulation-and-on-the-california-consumer-privacy-act-of-2018-which-was-influenced-by-the-european-legisl/

[36] International Association of Privacy Professionals, "IAPP-EY Annual Governance Report 2018."

[37] Hosuk Lee-Makiyama, "The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Its Costs," in Protection of Information and the Right to Privacy—A New Equilibrium?, ed. Luciano Floridi (Springer, 2014), 85–94.

In many respects, the CCPA seeks to emulate the GDPR characteristics, thus having the potential to cause similar effects in the US.

While the purpose of the GDPR was to regulate the processing of personal data and enhance data governance, a closer look suggests that we should be wary of its serious and negative unintended consequences.

Evidence shows that such top-down legislative efforts are concerning since their design requirements seem to encourage compliance rather than security. Additionally, their requirements can become rapidly outdated, increasing the possibility of stunting innovation that can lead to superior, more consumer-centric governance systems.

B. Alternatives

Although scientific research on data protection and privacy suggests that consumer education and privacy enhancing technologies are essential to creating trust online,[38] these inputs are ignored in both top-down approaches discussed in this paper.

Specific policy alternatives which have been evidenced to provide superior governance outcomes are privacy enhancing technologies, consumer education, and standard setting promulgating industry best practices.

Innovative privacy enhancing technologies, for example, have shown to provide a more flexible, innovation-based approach, yielding software and systems that are better

[38] Layton, Roslyn, and Julian McLendon. "The GDPR: What It Really Does and How the US Can Chart a Better Course. Fed." Soc. Rev 19 (2018): 234-248.

designed to protect data and privacy and empowering firms to operate with data protection as a competitive characteristic.[39] While there are already hundreds of privacy-enhancing technologies,[40] no one particular technology is best for all companies.

Providing and facilitating instructive and robust consumer education should be a key public policy priority. After all, consumers are key stakeholders and an integrative part of the IoT governance ecosystem. As such, consumers should proactively engage in reducing security threats as well. Before we get too excited by the flashy features of a new IoT gadget, as consumers we must not overlook basic security protocols.

Cyber hygiene education and consumer literacy efforts can help arm IoT device consumers with beneficial information and help them make better informed decisions. Journalists and cybersecurity researchers can also draw additional consumer attention to companies' errant behavior. For example, as a result of public pressure, a Chinese company whose webcams were leveraged in the Mirai botnet decided to recall millions of devices.[41]

Policy should support the innovation of new and better privacy and cybersecurity enhancing voluntary frameworks and standards. Basic privacy and cyber practices can include adopting industry best practices or voluntary standards such as the US National

[39] Kenneth A. Bamberger and Deirdre K. Mulligan, "Privacy on the Ground: Driving Corporate Behavior in the United States and Europe," 2015.
[40] Roslyn Layton, "Statement Before the Federal Trade Commission on Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201, Market Solutions of Online Privacy," August 20, 2018.
[41] Michael Mimoso, "Chinese Manufacturer Recalls IOT Gear Following Dyn DDoS," Threat Post, October 24, 2016, https://threatpost.com/chinese-manufacturer-recalls-iotgear-following-dyn-ddos/121496/

Institute of Standards and Technology (NIST) Framework for improving critical infrastructure cybersecurity.[42] These policy tools have the capability to further fill the governance gap.

Privacy enhancing technologies, consumer education, and standard setting promulgating industry best practices are only a few of the examples of governance that have the capability to show that multistakeholder arrangements can achieve sustainable long-term management in the IoT ecosystem.

When considering governance alternatives, it is critical to note that the IoT ecosystem is driven by change and interaction, and it is necessarily dynamic.[43] As a result, top-down static approaches treating privacy and cybersecurity as market failures in need of government correction downplay innovative market solutions that have the potential to deliver superior privacy and cybersecurity governance (e.g. cyber insurance, certification programs, or superior and cheaper methods of detecting malware).

The US should not copy the regulatory approach implemented in the EU. Instead, it can fundamentally improve on the GDPR by fostering a multistakeholder governance approach that promote efforts to mitigate cyber risk and privacy issues and align incentives to improve the ecosystem as a whole. This would ultimately provide a more flexible approach that promotes privacy and cybersecurity without hampering

[42] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," January 10, 2017, https://www.nist.gov/sites/default/files/documents/draft-cybersecurity-framework-v1.11.pdf

[43] Anne Hobson. "The Resilience Approach to Cybersecurity Policy in the Internet of Things Ecosystem." July 2019, Policy Paper 2019.004, Center for Growth and Opportunity.

innovation, empowers consumers to make informed decisions, and ensures innovators and entrepreneurs the freedom to invent privacy- and security- enhancing technologies.

Conclusion

The IoT ecosystem is characterized by its complex, dynamic, decentralized and distributed nature. With innovation in self-driving automobiles, medical electronics and other Internet of Things devices continuing to be primarily built on a core of open source code, leaves this technology vulnerable to hacks that could have life-threatening consequences. In light of these risks, companies that knowingly and unknowingly use out-of-date and unsecure open source components must be more diligent in countering these threats.

Given IoT pervasiveness, placing the responsibility for security on the communication component alone is insufficient. Yet, we need to be cautious when it comes to the efficiency and trade-offs of top-down strict regulatory approaches. While clear guidelines are important for providing innovators with regulatory certainty, a more flexible IoT governance approach engaging a multitude of stakeholders (industry, governments, consumers, and civil-society) is more promising to enhance privacy and cybersecurity in the IoT ecosystem while building resilience in the ecosystem without discouraging innovation.