Technological Convergence: Regulatory, Digital Privacy, and Data Security Issues

May 30, 2019

Congressional Research Service
https://crsreports.congress.gov
R45746

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R45746

May 30, 2019

Suzy E. Park
Analyst in Science and Technology Policy

Technological Convergence: Regulatory, Digital Privacy, and Data Security Issues

Technological convergence, in general, refers to the trend or phenomenon where two or more independent technologies integrate and form a new outcome. One example is the smartphone. A smartphone integrated several independent technologies—such as telephone, computer, camera, music player, television (TV), and geolocating and navigation tool—into a single device. The smartphone has become its own, identifiable category of technology, establishing a $350 billion industry.

Of the three closely associated convergences—technological convergence, media convergence, and network convergence—consumers most often directly engage with technological convergence. Technological convergent devices share three key characteristics. First, converged devices can execute multiple functions to serve blended purpose. Second, converged devices can collect and use data in various formats and employ machine learning techniques to deliver enhanced user experience. Third, converged devices are connected to a network directly and/or are interconnected with other devices to offer ubiquitous access to users.

Technological convergence may present a range of issues where Congress may take legislative and/or oversight actions. Three selected issue areas associated with technological convergence are regulatory jurisdiction, digital privacy, and data security. First, merging and integrating multiple technologies from distinct functional categories into one converged technology may pose challenges to defining regulatory policies and responsibilities. Determining oversight jurisdictions and regulatory authorities for converged technologies can become unclear as the boundaries that once separated single-function technologies blend together. A challenge for Congress may be in delineating which government agency has jurisdiction over various converged technologies. Defining policies that regulate technological convergence industry may not be simple or straightforward. This may further complicate how Congress oversees government agencies and converged industries due to blending boundaries of existing categories.

Second, converged technologies collect and use personal and machine data which may raise digital privacy concerns for consumers. Data collection and usage are tied to digital privacy issues because a piece or aggregation of information could identify an individual or reveal patterns in one's activities. Converged or smart technologies leverage large volumes of data to try to improve the user experience by generating more tailored and anticipatory results. However, such data can potentially identify, locate, track, and monitor an individual without the person's knowledge. Such data can also potentially be sold to third-party entities without an individual's awareness. As the use of converged technologies continues to propagate, digital privacy issues will likely remain central.

Third, data security concerns are often associated with smart devices' convenient ubiquitous features that may double as vulnerabilities exploited by malicious actors. Data security, a component of cybersecurity, protects data from unauthorized access and use. Along with digital privacy, data security is a pertinent issue to technological convergence. As converged devices generate and consume large volumes of data, multiple data security concerns have emerged: potentially increased number of access points susceptible to cyberattacks, linkage to physical security, and theft of data.

Relatively few policies are in place for specifically overseeing technological convergence, and current federal data protection laws have varied privacy and data security provisions for different types of personal data. To address regulatory, digital privacy, and data security issues, Congress may consider the role of the federal government in an environment where technological evolution changes quickly and continues to disrupt existing regulatory frameworks. Regulating technological convergence may entail policies for jurisdictional deconfliction, harmonization, and expansion to address blended or new categories of technology. One approach could be for Congress to define the role of federal government oversight of digital privacy and data security by introducing

new legislation that comprehensively addresses digital privacy and data security issues or by expanding the current authorities of federal agencies. When considering new legislation or expanding the authorities of federal agencies, three potential policy decisions are (1) whether data privacy and data security should be addressed together or separately, (2) whether various types of personal data should be treated equally or differently, and (3) which agencies should be responsible for implementing any new laws.

Contents

Figures

Contacts

Introduction

Technological convergence, in general, refers to the trend or phenomenon where two or more independent technologies integrate and form a new outcome. One example is the smartphone. A smartphone integrates several independent technologies—such as telephone, computer, camera, music player, television (TV), and geolocating and navigation tool—into a single device. The smartphone has become its own, identifiable category of technology. Currently, over 35% of the global population are smartphone users and over 3 billion active devices are in circulation.[1] In the United States, about 80% of the U.S. population are smartphone users, and over 280 million active devices are in circulation.[2] The technological convergence has resulted in establishing a new and prominent smartphone industry sector, worth over $350 billion globally, according to some estimates.[3]

Technological convergence may present a range of issues where Congress may take legislative and/or oversight actions. Three selected issue areas associated with technological convergence are regulatory jurisdiction, digital privacy, and data security. First, merging and integrating multiple technologies from distinct functional categories into one converged technology may pose challenges to defining regulatory policies, roles, and responsibilities. Determining oversight jurisdictions and regulatory authorities for converged technologies may become complicated as the boundaries that once separated single-function technologies are blended together. In other words, delineating which policy authorizes which government agency to apply which standards to regulate which industry is no longer simple and straightforward. How Congress chooses to oversee certain industries and government agencies may also become complicated due to converging technologies that blur and blend existing categorical boundaries.

Second, digital privacy concerns stem from converged technologies' collection and usage of personal and machine data.[4] Technological convergence facilitates increasing consumption and collection of data, which poses potential digital privacy concerns for consumers. Data collection and usage are tied to digital privacy issues because a piece or aggregation of information could identify an individual or reveal patterns in their activities. Converged technologies leverage large volumes of data to try to improve the user experience by generating more tailored and anticipatory results. This data can also potentially be used to identify, locate, track, and monitor an individual without the person's knowledge. The same data can potentially be sold to third-

[1] Statista, "Smartphone Penetration Worldwide 2014-2021," https://www.statista.com/statistics/203734/global-smartphone-penetration-per-capita-since-2005/.

Statista, "Global Smartphones Installed Base 2008-2017 | Statistic," https://www.statista.com/statistics/371889/smartphone-worldwide-installed-base/.

[2] Statista, "Smartphone Penetration United States 2017-2023 | Statistic," https://www.statista.com/statistics/201184/percentage-of-mobile-phone-users-who-use-a-smartphone-in-the-us/.

Statista, "Smartphones Installed Base in the US 2013-2022 | Statistic," https://www.statista.com/statistics/619838/smartphones-installed-base-in-the-us/.

[3] Statista, "Global Smartphone Revenue 2011-2018 | Statistic," https://www.statista.com/statistics/687476/global-smartphone-revenues/.

Arjun Kharpal, "6 Billion Smartphones Will Be in Circulation in 2020: Report," *CNBC*, January 17, 2017, https://www.cnbc.com/2017/01/17/6-billion-smartphones-will-be-in-circulation-in-2020-ihs-report.html.

[4] Personal data refers to information that pertains to a specific individual person. Examples of personal data include name, social security number, email address, phone number, home address, fingerprints, and genetics information. Machine data refers to information generated by a machine—such as a computer, application, sensors, or a device—based on operational activities. Examples of machine data include sensor readings, network data for communication protocols, and web logs.

party entities without an individual's awareness. As the use of converged technologies continues to propagate, digital privacy issues will likely remain central to the policy debate.

Third, data security concerns are often associated with smart devices.[5] As devices are able to interconnect, the convenient ubiquitous features may create vulnerabilities that could be exploited by malicious actors. Data security, a component of cybersecurity, protects data from unauthorized access and use. Along with digital privacy, data security is a pertinent issue for converged technologies, which generate and consume large volumes of data. Technological convergence poses three potential data security concerns: increased number of access points susceptible to cyberattacks, linkage to physical security, and theft of data.

The first section of this report describes technological convergence along with closely associated media convergence and network convergence. The report uses the Internet of Things (IoT) and smart home devices as primary examples.[6] Of these three convergences, consumers most often directly engage with converged technologies. In contrast, general consumers may not have the same level of engagement or understanding of media and network convergences, as they often occur in the background.

The second section of this report presents regulatory, digital privacy, and data security issues pertaining to technological convergence. The current state, challenges, and recent legislative activities are discussed.

The third section of this report concludes with potential considerations for Congress. An overarching consideration for regulatory, digital privacy, and data security issues may be determining the role, if any, of the federal government in an environment where technological evolution changes quickly and continues to disrupt existing frameworks. Policies governing these three issues—regulations, digital privacy, and data security—may be of interest to Congress as well as other stakeholders, including U.S. government agencies, commercial entities, and the general public.

Description of Technological Convergence

"Technological convergence" is a concept whereby merging, blending, integration, and transformation of independent technologies leads to a completely new converged technology. This broad, complex concept encompasses a wide range of technologies, including IoT and smart home devices. When a converged technology emerges, it often replaces single-function technologies or renders them obsolete. In this sense, technological convergence can be viewed as a progression or evolution of technology.[7]

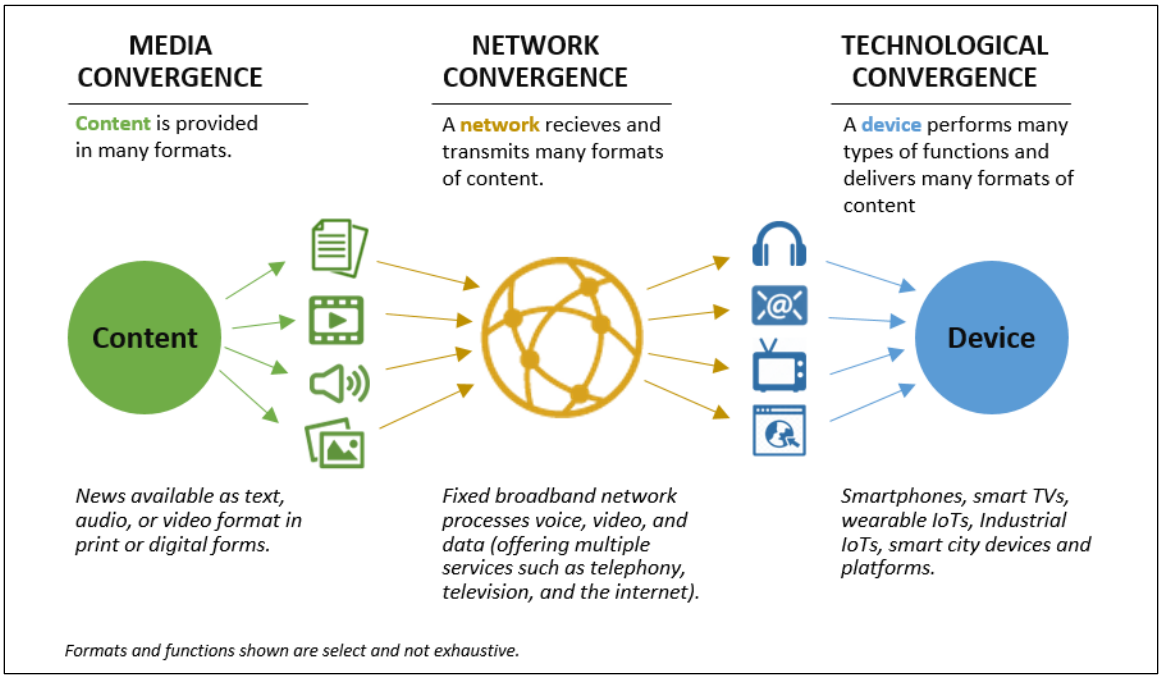
[5] Many technological convergence devices are called "smart" devices, which are electronic devices that have sensors and are connected to a network and/or other devices for sharing information and interacting with users. Sophisticated smart devices have machine learning algorithms that offer the ability to learn from past data and user preferences.

[6] Media convergence refers to content that is made available through multiple forms, formats, and access points on multiple platforms. Network convergence refers to a single network infrastructure that handles and distributes multiple types of media. The IoT is a system of interrelated devices that transfer data over a network among connected devices without requiring human-to-human or human-to-computer interaction. These topics are further discussed in subsequent sections of this report.

[7] Dong Hee Shin, Won-Yong Kim, and Dong-Hoon Lee, "Convergence Technologies and the Layered Policy Model: Implication for Regulating Future Communications," in *Annual Meeting* (International Communication Association, United States: International Communication Association, 2006), http://web.b.ebscohost.com/ehost/detail/detail?vid=3&sid=00dd6275-99fe-4a5a-a32d-4ccb6b08620c%40pdc-v-sessmgr03&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=27203990&db=ufh.

A discussion of technological convergence in isolation is difficult because technological convergence is closely associated with media convergence and network convergence. Technological, media, and network convergences are interdependent, but each possesses subtle distinctions. These three terms are often used interchangeably, further complicating the discussion of an already complex topic. **Figure 1** illustrates relationships between technological, media, and network convergences.

Figure 1. Technological, Media, and Network Convergences



Source: CRS.

Technological convergence: This occurs when the *functions* of different technologies are merged and interoperate as a single unit. A converged unit can typically process multiple types of media that correspond to each technology that merged. Technological convergence includes devices and systems that interface with end users. For example, a user interacts with converged devices, such as a smart television (TV), to access the contents that are distributed over a network. A smart TV has combined the functions of a traditional TV, a computer, and several other devices that used to have one specific purpose. In addition to displaying over-the-air broadcast TV channels, smart TVs interface with users to surf the internet, view photos taken from smartphones and stored in the "cloud," display feeds from home security cameras connected to a network, play music, notify users of incoming calls and messages, and allow video teleconferencing.[8] Smart TVs can process a variety of formats of media to perform multiple functions.

Media convergence: This refers to *content* that is made available through multiple forms, formats, and access points. Media convergence proliferated as analog mediums of communication

[8] Cloud storage refers to storing digital data on remote servers and accessing the data through the internet. Because data are not stored in a single, fixed, isolated location, and can be accessed from anywhere, cloud storage gives the impression of storing data on a non-concrete, flexible, fluid, mobile "cloud."

became digitized. For example, the contents on a newspaper used to be available only in print. The same content is currently available in both print and digital forms, as text, visual, and/or audio formats, and through multiple devices and platforms including social media.

Network convergence: This refers to a single *network infrastructure* that handles and distributes multiple types of media. Network convergence became prominent when telecommunications and information networks integrated; it became prevalent when mobile cellular communications incorporated access to the internet and made it widespread. For example, today's cable companies process information in forms of voice, video, and data on a single network and often offer their services as a bundle package (e.g., phone, television, and internet services). Similarly, cellular networks, which distribute information to and from mobile devices and fixed platforms, process voice, video, and data.

Prior to network, media, and technological convergences, a separate, independent network was dedicated to handling and distributing one particular type of media that was processed by a single-function device. For example, a telephone network distributed audio information (i.e., voice) between telephone handsets. A broadcasting network delivered video to television sets. Convergence removes such pairing (i.e., "decouples") between media, network, and device.[9] Decoupling gives convergence its versatility, flexibility, and complexity.

Characteristics of Smart Devices

Many technological convergence devices are called "smart" devices, which often include IoT devices. (Examples of IoT devices are discussed in following sections.) Despite a wide range of applications, smart converged technologies share key characteristics:

- Smart devices can execute multiple functions to serve blended purposes;
- Smart devices can collect and use data in various formats and employ machine learning algorithms[10] to deliver optimized and enhanced user experience; and
- Smart devices are connected to a network directly and/or are interconnected with other smart devices, offering ubiquitous access to users from anywhere on any platform.

These key characteristics may present potential policy questions for Congress, including the following:

- Who will provide oversight and how will regulatory authorities be applied to technologies that serve multiple functions or that do not belong to an established category?

[9] Corinna Peil and Sergio Sparviero, "Media Convergence Meets Deconvergence," in *Media Convergence and Deconvergence*, ed. Sergio Sparviero, Corinna Peil, and Gabriele Balbi, Global Transformations in Media and Communication Research—A Palgrave and IAMCR Series (Cham: Springer International Publishing, 2017), 3–30, https://doi.org/10.1007/978-3-319-51289-1_1.

[10] Machine learning algorithms examine historical information and user preferences, extract patterns, and attempt to predict or anticipate a user's need. The predictive capability improves with more historical data and iterations of adjusting rules or model parameters. According to the Merriam-Webster dictionary, an algorithm is "a procedure for solving a mathematical problem (as of finding the greatest common divisor) in a finite number of steps that frequently involves repetition of an operation." Many different mathematical principles form the basis of machine learning algorithms, executed as a software program that leverage computing power and executes functions without explicit commands.

- How should consumer data be collected and used to protect digital privacy without limiting technology innovation?
- How to shape data security practices to safeguard personal information and physical security from malicious actors?

An Overview of Internet of Things

The IoT is a common example of technological convergence. The IoT is a system of devices that are connected to a network and each other, exchanging data without necessarily requiring human-to-human or human-to-computer interaction.[11] In other words, IoT is a collection of electronic devices that can share information among themselves (e.g., smart home devices). The IoT possess all three characteristics of converged technologies: multiple functions, data collection and use, and ubiquitous access. Various categories of IoT include industrial Internet of Things, Internet of Medical Things, smart city infrastructures, and smart home devices.

IoT industry is a growing market both globally and in the United States.[12] According to some estimates, in 2018, the IoT retail market in the United States was almost $4 billion,[13] and over 700 million consumer IoT devices were in use in 2017 in the United States.[14] **Figure 2** illustrates global revenue of the IoT from 2012 to 2018, according to Statista, a company that consolidates statistical data, based on information from IC Insights.[15] In 2018, consumer IoT devices, such as wearable and connected smart home devices, generated over $14 billion globally. The connected cities category, or smart cities, was the largest (41%) of 2018 global IoT revenue. The industrial Internet of Things, such as smart factories, had the biggest growth in terms of global revenue between 2017 and 2018 among the different categories of the IoT. An estimate of various IoT markets by McKinsey also shows the industrial IoT as potentially increasing the most by 2025 compared to other IoT systems.[16] The development, application, and usage of IoT will likely continue to grow with Fifth-Generation (5G) Technologies cellular service, which will allow a

[11] Samuel Greengard, *The Internet of Things*, The MIT Press Essential Knowledge Series (Cambridge, Massachusetts: The Massachusetts Institute of Technology Press, 2015).

IoT Agenda, "What Is Internet of Things (IoT)?—Definition from WhatIs.Com," https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[12] Statista, "IoT Market Size Worldwide 2016-2020 | Statistic," https://www.statista.com/statistics/764051/iot-market-size-worldwide/.

Daniel Alsen, Mark Patel, and Jason Shangkuan, "The Future of Connectivity: Enabling the Internet of Things," McKinsey and Company, https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/the-future-of-connectivity-enabling-the-internet-of-things.

Statista, "IoT Infrastructure Market by Application in US 2016-2024 | Statistic," https://www.statista.com/statistics/761278/iot-infrastructure-market-by-application-in-us/.

[13] Statista, "IoT Hardware in US Retail Market 2014-2025 | Statistic," https://www.statista.com/statistics/688756/iot-in-retail-market-in-the-us/.

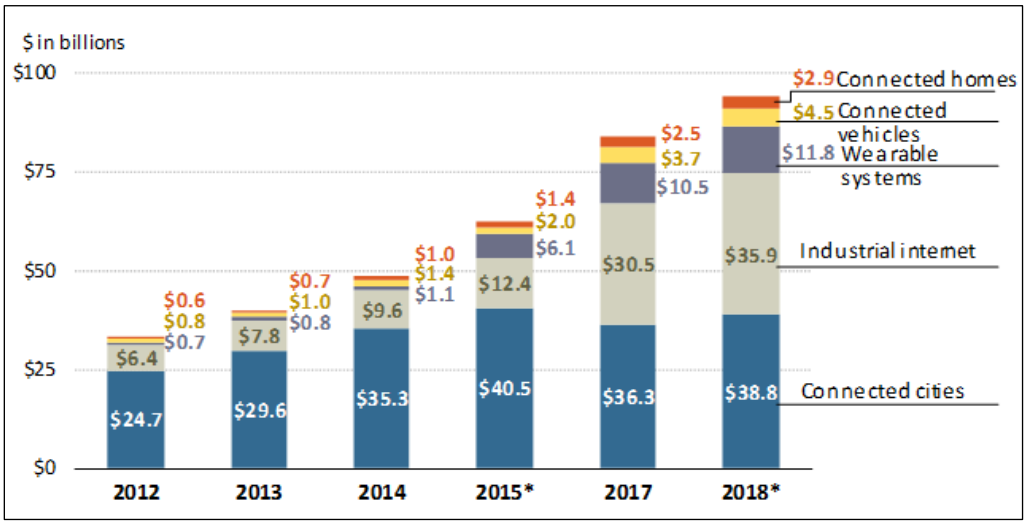
[14] Statista, "IoT Devices in Use by Category in US 2017 | Statistic," https://www.statista.com/statistics/757717/iot-consumer-product-installed-base-in-the-us-by-category/.

[15] Statista, "IoT Subsystems Revenue Worldwide 2012-2018 | Statistic," https://www.statista.com/statistics/503466/iot-subsystems-revenue-worldwide/.

[16] James Manyika et al., "Unlocking the Potential of the Internet of Things," McKinsey and Company, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

larger number of devices to be connected simultaneously to a network, supporting not only consumer but industrial use of IoT devices and systems.[17]

Figure 2. Internet of Things Subsystems Revenue Worldwide from 2012 to 2018



Source: CRS created based on data from Statista, "IoT Subsystems Revenue Worldwide 2012-2018 | Statistic," https://www.statista.com/statistics/503466/iot-subsystems-revenue-worldwide/.

Notes: The source for this figure did not have the information for 2016 and applied estimations for 2015 and 2018 (with *). The Connected cities category refers to smart cities; the Industrial internet category refers to industrial internet of things; the Wearable systems category includes consumer devices that register and provide personal health information; and the Connected homes category refers to smart homes.

IoT devices are used in many different fields and serve a variety of functions. The IoT encompasses a broad range of applications. Selected categories of IoT devices are discussed below.

Industrial Internet of Things (IIoT): Examples of commercial application of the IoT can be found in the manufacturing industry. Referred to as industrial Internet of Things (IIoT), networked machines in a production facility can communicate and share information to improve efficiency, productivity, and performance.[18] The application of IIoT can vary significantly, from detecting corrosion inside a refinery pipe to providing real-time production data.[19] Also, IIoTs can enable a variety of industries, such as manufacturing, chemicals, food and beverage, automotive, and steel, to transform their operations and potentially yield financial benefits.[20] Currently in North America, there are more consumer IoT connections than IIoT connections, but this may

[17] CRS Report R45485, *Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress*, by Jill C. Gallagher and Michael E. DeVine.

[18] Lea Bolz, Heike Freund, Tarek Kasah, and Bodo Koerber, "IIoT Platforms for Industrial Equipment and Machinery Players," McKinsey and Company, https://www.mckinsey.com/industries/advanced-electronics/our-insights/iiot-platforms-the-technology-stack-as-value-driver-in-industrial-equipment-and-machinery.

[19] GE Digital, "Everything You Need to Know about IIoT," https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-internet-things.

[20] Ibid.

change in the future.[21] Incorporation of IIoT and analytics is considered by some as the Fourth Industrial Revolution (4IR).[22]

Internet of Medical Things (IoMT): Some experts project the use of Internet of Medical Things (IoMT) is increasing.[23] IoMT devices, such as heart monitors and pace makers, collect and send a patient's health statistics over various networks to healthcare providers for monitoring, remote configuration, and preventions. In 2017, over 300 million IoT devices in the medical sector were connected worldwide, and, in 2018, over 400 million devices were connected.[24] At a personal health level, wearable IoT devices, such as smart watches and fitness trackers, can track a user's physical activities, basic vitals, and sleeping patterns. In 2017, over 40 million fitness tracker IoT were in use in the United States.[25]

Smart Cities: IoT devices and systems in transportation, utilities, and infrastructure sectors may be grouped under the category of "smart city."[26] An example of utilities IoT in a smart city is "smart" grid and meters for electricity, water, and gas where sensors collect and share customer usage data to enable the central control system to optimize production and distribution to meet demand real-time.[27] An example of transportation IoT in a smart city is fare readers and status trackers or locaters that interface across all public transportation platforms.[28] Columbus, OH's winning proposal for the Department of Transportation's (DOT) Smart City Challenge of 2016, included connected infrastructure that interacts with vehicles, trip planning and common payment system across multiple transit system, and electric autonomous vehicles and shuttles.[29] Other finalists of the DoT Smart City Challenge were Austin, TX; Denver, CO; Kansas City, MO; Pittsburgh, PA; Portland, OR; and San Francisco, CA.[30] Smart cities is currently the largest segment of IoT in terms of revenue.[31]

Smart Home: Consumer product IoT devices used in homes and buildings are often grouped under the "smart home" category. Included in this categories are smart appliances, smart TV, smart entertainment systems, smart thermostats, and network-connected light bulbs, outlets, door

[21] Statista, "IoT Connections North America 2017-2025 | Statistic," https://www.statista.com/statistics/933099/iot-connections-north-america/.

[22] PricewaterhouseCoopers, "4IReady," https://www.pwc.com/us/en/library/4ir-ready.html.

[23] Bernard Marr, "Why the Internet of Medical Things (IoMT) Will Start to Transform Healthcare in 2018," *Forbes*, https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/.

[24] Statista, "Global Connected IoT Devices by Sector 2017 and 2018 | Statistic," https://www.statista.com/statistics/748737/worldwide-connected-iot-devices-by-sector/.

[25] Statista, "IoT Devices in Use by Category in US 2017 | Statistic," https://www.statista.com/statistics/757717/iot-consumer-product-installed-base-in-the-us-by-category/.

[26] "Smart Cities and Artificial Intelligence," *Brookings* (blog), January 25, 2019, https://www.brookings.edu/events/smart-cities-and-artificial-intelligence/.

[27] Andrew Meola, "IoT for Utilities: Smart Water, Gas and Electric Utilities Coming Soon," *Business Insider*, https://www.businessinsider.com/internet-of-things-utilities-water-electric-gas-2016-10.

[28] U.S. Department of Transportation, "Smart City Challenge," September 28, 2016, https://www.transportation.gov/smartcity.

[29] Smart Columbus, "Home | SmartColumbus," https://smart.columbus.gov; U.S. Department of Transportation,"The Winner: Columbus, Ohio," September 28, 2016, https://cms.dot.gov/smartcity/winner.

[30] U.S. Department of Transportation, "Round Two: Seven Finalists Create Plans To Implement Their Visions," September 28, 2016, https://cms.dot.gov/smartcity/7-finalists-cities.

[31] Statista, "IoT Subsystems Revenue Worldwide 2012-2018 | Statistic," https://www.statista.com/statistics/503466/iot-subsystems-revenue-worldwide/.

locks, door bells, and home security systems.[32] These smart home IoT devices are connected to a single network and can be controlled remotely over the internet. Eight of 11 categories of consumer IoT devices used in 2017 were related to smart home.[33] In 2018, the size of the global smart home market was estimated to be over $30 billion.[34]

An Example: Smart Home

A smart home contains a collection of consumer IoT devices intended for personal use where user experience is improved by connecting various features of a house to a network. For example, smart home IoT devices may be interconnected to each other and to a central control system for a home with voice interface, often referred to as a virtual assistant. Commonly known examples of virtual assistants are Amazon's Alexa, Apple's Siri, Google Assistant, Microsoft's Cortana, and Samsung's Bixby. A virtual assistant is a platform that can manage and relay information to smart home devices based on user-established criteria.

Moreover, a smart home may have a doorbell with a video camera and a speaker that allows a user to see who is at the door and to speak to the person at the door from anywhere over the internet. A smart home may have a smart door lock that can be locked and unlocked remotely. In addition, the thermostat, lights, electrical outlets, and appliances in a smart home may be remotely controlled by a user over the internet. A smart appliance, such as a smart refrigerator that is networked, can use its sensors to identify items and can notify a user based on set criteria, such as restocking alerts or suggested recipes.

Some smart home devices resemble traditional devices, but with cross-over functions or networking abilities. Examples include smart lightbulbs, smart electrical outlet plugs, smart TV, and smart appliances. Some smart home devices are establishing a new category of industry segment that did not exist previously. An example is Amazon's Echo products with virtual assistant Alexa as voice user interface. Whether it is the former (evolutionary technologies) or the latter (new/revolutionary technologies), the smart home industry is fast emerging and growing.[35]

Smart home devices, which are a type of IoT, possess the three characteristics of converged technologies: multiple or blended functions, collection and use of data, and ubiquitous access through network connection. Thus, potential policy interests associated with technological convergence can be also observed in smart home devices. Potential smart home issues for Congress include the following.

Congress may decide it is necessary to resolve oversight jurisdictions and regulatory authorities of smart home devices, especially for products like virtual assistants, which may not belong to an established category of technology. The mission of the Federal Trade Commission (FTC) includes both protecting consumers and promoting business competition.[36] Congress may choose to review

[32] Statista, "Smart Home—Worldwide | Statista Market Forecast," https://www.statista.com/outlook/279/100/smart-home/worldwide.

[33] Statista, "IoT Devices in Use by Category in US 2017 | Statistic," https://www.statista.com/statistics/757717/iot-consumer-product-installed-base-in-the-us-by-category/.

[34] Statista, "Global Smart Home Market Size 2016-2022 | Statistic," https://www.statista.com/statistics/682204/global-smart-home-market-size/.

Market size is different from revenue. Market size is the potential revenue—an estimated, possible, total income that can be generated from all potential customers, which compose a segment of a market. Revenue is the total positive cash flow from sales of goods or services in a given timeframe.

[35] Statista, "Smart Home Report 2019," https://www.statista.com/study/42112/smart-home-report/.

[36] Federal Trade Commission, "What We Do," June 7, 2013, https://www.ftc.gov/about-ftc/what-we-do.

the FTC's current authorities to ensure that they are sufficient to oversee emerging smart home technologies. In addition, potentially deconflicting or harmonizing jurisdictions may be discussed if other federal government organizations and their mission are impacted by emerging smart home technologies.

Congress may decide that new or expanded policies are necessary to protect consumer digital privacy, including personal data that are collected and used by smart home devices, such as a smart TV, in private spaces, such as a user's home. Although the FTC does promote a level of digital privacy through its consumer protection authorities, emerging digital privacy issues are linked to practices that are legal as opposed to fraud, theft, or other malicious activities.[37] Congress may examine whether a federal law that comprehensively addresses personal digital privacy is necessary or an expansion of the FTC's consumer data protection authorities is required.

Emerging smart home technologies may further necessitate safeguarding data from malicious actors. In addition to collecting and using personal data, smart home devices bridge physical security and cybersecurity. Malicious actors may have more means to exploit a user's information and home through smart home devices, which offer ubiquitous access as a key convenience feature. Whether current policies adequately addresses data, cyber, and physical security concerns may also be considered.

Selected Issues Associated with Technological Convergence

Regulation, digital privacy, and data security are three selected issues associated with technological convergence that may be of interest to many stakeholders, including Congress. As identified in the smart home example in the previous section, each of these three issues is discussed further in subsequent subsections. The three selected issues are tied to the three characteristics of converged technologies discussed previously in the "Characteristics of Smart Devices" section. First, convergence of technologies blend and blur existing categorical distinctions for each technology because a converged technology can perform multiple functions. Second, technological convergence consumes, collects, and generates a large volume of both personal and machine data. Third, converged technologies allow ubiquitous access points to the end users.[38] These characteristics are typically observed as a result of decoupling the devices from media and network.

Regulatory Issues

Congress may consider policies that address blending standards and boundaries as converged technologies and companies merge and replace traditionally independent and distinct categories. Policy issues may include oversight jurisdictions, regulatory authorities, and commercial competitiveness since a converged technology could fall within multiple domains. An example

Federal Trade Commission, "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority," June 7, 2013, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[37] Federal Trade Commission, "Data and Visualizations," October 15, 2018, https://www.ftc.gov/enforcement/data-visualizations.

[38] Ubiquitous access refers to the capability of remotely accessing a device of a system anytime, from anywhere on any platform.

may be delineating the Federal Communications and Commission's (FCC) and the FTC's authorities on convergence technologies as more devices and services become mobile and wirelessly connected.[39]

Merging and integrating multiple technologies from distinct functional categories into one converged technology pose challenges to regulatory policies and responsibilities. Determining oversight jurisdictions and regulatory authorities for converged technologies becomes unclear as the boundaries that once separated single-function technologies blend and blur together. A challenge for policymakers may be in delineating which government agency and which policies and standards would best apply to certain technologies or certain industries. Where there were once clear lines of authority by industry or media type (e.g., voice, video, data), they are no longer simple and straightforward for technologies where these functionalities have converged. How Congress oversees which industries and government agencies may become complicated due to converging technologies that blend existing categorical boundaries. Congress may decide that it is necessary for specific legislative committees to effectively oversee a converged technology that serves multiple functions. As a result, the alignment of converged technologies to regulatory authorities may shift as technologies evolve.

The complexities in setting regulatory jurisdiction can be further subdivided into regulating converging *technologies* and regulating evolving technology *companies*. They are discussed below.

Regulating Converging Technologies

Regulating a converging technology, which is a result of blending or integrating multiple technologies, can be challenging. This is because (1) the one-to-one relationship between a converging technology and a regulatory entity is no longer clear, and (2) a converging technology may create a new sector where a regulatory entity has not been identified.

Initially, the standards and oversight policies for a specific technology were established independently. They were not necessarily developed with merging or interoperability in mind. For example, telephony (when providing voice), cable TV (when providing video), and mobile cellular technologies each follow their respective standards, and these services were regulated by policies specific to each type. When a converged technology utilizes differing communications technologies, it may be required to adhere to multiple standards and regulations.

In such cases, multiple agencies may need to regulate a single converged technology. This may require extended timelines for regulatory reviews. Industry may incur additional costs to meet standards and reporting requirements for converged technologies.

In other situations, as technologies converge, the outcome may yield a completely new technology for which a regulatory category did not previously exist. Examples include social media, IoTs, and virtual assistants. Without a clear regulatory and oversight framework in place, new converged technologies may be left unregulated, partially regulated, or regulated under a newly developed framework. They could also be left to self-regulate by the industry; or they could be overlooked as governing bodies remain indeterminate on which jurisdictional boundaries need to be stretched to cover emerging technology fields.

[39] CRS In Focus IF10955, *Access to Broadband Networks: Net Neutrality*, by Angele A. Gilroy.

Regulating Evolving Companies

Regulating companies that offer converged technologies is challenging because the services and product lines evolve and expand such that they do not fall within a single category. Although diversification is considered normal business practice, technological convergence broadens the operational range for companies, spanning multiple industry sectors. Antitrust concerns could arise, or companies may not be subjected to the same level of oversight and regulation due to lack of classification.

For example, companies such as Amazon, Apple, and Google each offer smart home devices and platforms. Some of these devices, such as a smart doorbell with a video camera, smart doors and locks, and networked contact sensors and video cameras, may function as home security devices. Many of these products are bundled as a starting kit for home security. However, these technology convergence companies may not be required to follow state and local regulations as traditional home security companies that provide monitored security service do.[40]

Another example discussed widely in Congress is social media—whether social media companies should be classified as information technology companies, as advertising and marketing firms, as communications platforms, or as the press. As converged technologies and associated companies straddle or fall between jurisdictional boundaries, regulatory roles and responsibilities become more complex.

Digital Privacy Issues

Congress may be interested in digital privacy concerns of converged technologies, which often collect and use personal information and machine data as they directly interface with end-users. Current federal laws protect certain types of data pertaining to privacy by specifying collection, storage, use, and dissemination practices. As converged technologies generate and innovatively leverage more types and volumes of data that can identify, locate, or track a person, consumer concerns for protecting digital privacy may intensify.

Technological convergence facilitates increased consumption and collection of data, posing potential digital privacy concerns for consumers. Data collection and usage are tied to digital privacy issues because a piece or aggregation of information could identify an individual or reveal patterns in their activities. Converged technologies leverage large volumes of data to try to improve the user experience by generating more tailored and anticipatory results. However, such data can potentially identify, locate, track, and monitor an individual without the person's knowledge. As the use of converged technologies continues to propagate, digital privacy issues will likely remain central.

---

[40] Monitored security systems are actively observed by a professional home security company who take predetermined actions based on alerts and activities. Unmonitored or self-monitored security systems are managed by the user. Furthermore, professionally installed home security systems are set up by licensed technicians using equipment offered by a professional home security company. Do-it-yourself home security systems are installed by the user by purchasing a kit or sensor devices.

"What Organization Regulates Home Security Companies?," *SafeWise* (blog), https://www.safewise.com/home-security-faq/who-regulates-security-companies/; "What Is a Security System and How Does It Work?," *SafeWise* (blog), https://www.safewise.com/home-security-faq/how-do-security-systems-work/; "The Difference Between Monitored and Unmonitored Security Systems," *SafeWise* (blog), https://www.safewise.com/home-security-faq/monitored-unmonitored-systems/; and "Is a DIY Security System Better Than a Professionally Installed One?," *SafeWise* (blog), https://www.safewise.com/home-security-faq/diy-vs-professional/.

Current Data Protection Laws

While a federal law that comprehensively addresses digital privacy does not currently exist, many laws are in place to protect certain types of data and their impact on specific aspects of privacy. Current U.S. data protection laws include the following, as taken from CRS Report R45631, *Data Protection Law: An Overview*:[41]

> **Gramm-Leach-Bliley Act** (GLBA): The GLBA imposes several data protection obligations on financial institutions. These obligations are centered on a category of data called "consumer" "nonpublic personal information" (NPI), and generally relate to: (1) sharing NPI with third parties, (2) providing privacy notices to consumers, and (3) security NPI from unauthorized access.
>
> **Health Insurance Portability and Accountability Act** (HIPAA): Under the HIPAA, the Department of Health and Human Services (HHS) has enacted regulations protecting a category of medical information called "protected health information" (PHI). These regulations apply to health care providers, health plans, and health care clearinghouses (covered entities), as well as certain "business associates" of such entities. The HIPAA regulations generally speak to covered entities': (1) using or sharing of PHI, (2) disclosure of information to consumers, (3) safeguards for securing PHI, and (4) notification of consumers following a breach of PHI.
>
> **Fair Credit Reporting Act** (FCRA): The FCRA covers the collection and use of information bearing on a consumer's creditworthiness. FCRA and its implementing regulations govern the activities of three categories of entities: (1) credit reporting agencies (CRAs), (2) entities furnishing information to CRAs (furnishers), and (3) individuals who use credit reports issued by CRAs (users). In contrast to HIPAA or GLBA, there are no privacy provisions in FCRA requiring entities to provide notice to a consumer or to obtain his opt-in or opt-out consent before collecting or disclosing the consumer's data to third parties. FCRA further has no data security provisions requiring entities to maintain safeguards to protect consumer information from unauthorized access. Rather, FCRA's requirements generally focus on ensuring that the consumer information reported by CRAs and furnishers is accurate and that it is used only for certain permissible purposes.
>
> **The Communications Act**: The Communications Act of 1934 (Communications Act or Act), as amended, established the Federal Communications Commission (FCC) and provides a "comprehensive scheme" for the regulations of interstate communication. [T]he Communications Act includes data protection provisions applicable to common carriers, cable operators, and satellite carriers.
>
> **Video Privacy Protection Act** (VPPA): The VPPA was enacted in 1988 in order to "preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials." The VPPA does not have any data security provisions requiring entities to maintain safeguards to protect consumer information from unauthorized access. However, it does have privacy provisions restricting when covered entities can share certain consumer information. Specifically, the VPPA prohibits "video tape service providers"—a term that includes both digital video streaming services and brick-and-mortar video rental stores—from knowingly disclosing [personally identifiable information] (PII) concerning any "consumer" without that consumer's opt-in consent. The VPPA does not empower any federal agency to enforce violations or the Act and there are no criminal penalties for violations, but it does provide for a private right of action for persons aggrieved by the Act.

[41] CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh.

Family Educational Rights and Privacy Act (FERPA): The FERPA creates privacy protections for student education records. "Education records" are defined broadly to generally include any "materials which contain information directly related to a student" and are "maintained by an educational agency or institution." FERPA defines an "educational agency of institution" to include "any public or private agency or institution which is the recipient of funds under any applicable program." FERPA generally requires that any "educational agency or institution" (i.e., covered entities) give parents or, depending on their age, the student (1) control over the disclosure of the student's educational records, (2) an opportunity to review those records, and (3) an opportunity to challenge them as inaccurate.

Federal Securities Laws: While federal securities statutes and regulations do not explicitly address data protection, two requirements under these laws have implications for how companies prevent and respond to data breaches. First, federal securities laws may require companies to adopt controls designed to protect against data breaches. Second, federal securities laws may require companies to discuss data breaches when making required disclosures under securities laws.

Children's Online Privacy Protection Act (COPPA): The COPPA and the FTC's implementing regulations regulate the online collection and use of children's information. Specifically, COPPA's requirements apply to: (1) any "operator" of a website or online service that is "directed to children," or (2) any operator that has any "actual knowledge that it is collecting personal information from a child" (i.e., covered operators). Covered operators must comply with various requirements regarding data collection and use, privacy policy notifications, and data security.

Electronic Communications Privacy Act (ECPA): The ECPA was enacted in 1986, and is composed of three acts: the Wiretap Act, the Stored Communications Act (SCA), and the Pen Register Act. Much of ECPA is directed at law enforcement, providing "Fourth Amendment like privacy protections" to electronic communications. However, "ECPA's three acts also contain privacy obligations relevant to non-governmental actors. ECPA is perhaps the most compressive federal law on electronic privacy, as it is not sector-specific, and many of its provisions apply to a wide range of private and public actors. Nevertheless, its impact on online privacy has been limited. As some commentators have observed, ECPA "was designed to regulate wiretapping and electronic snooping rather than commercial data gathering," and litigants attempting to apply ECPA to online data collection have generally been unsuccessful.

Computer Fraud and Abuse Act (CFAA): The CFAA was originally intended as a computer hacking statute and is centrally concerned with prohibiting unauthorized intrusions into computers, rather than addressing other data protection issues such as the collection or use of data. Specifically, the CFAA imposes liability when a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains… information from any protected computer." A "protected computer" is broadly defined as any computer used in or affecting interstate commerce or communications, functionally allowing the statute to apply to any computer that is connected to the internet.

Federal Trade Commission Act (FTC Act): The FTC Act has emerged as a critical law relevant to data privacy and security. As some commentators have noted, the FTC has used its authority under the Act to become the "go-to agency for privacy," effectively filling in gaps left by the aforementioned federal statutes. While the FTC Act was originally enacted in 1914 to strengthen competition law, the 1938 Wheeler-Lea amendment revised Section 5 of the Act to prohibit a broad range of unscrupulous or misleading practices harmful to consumers. The Act gives the FTC jurisdiction over most individuals and entities, although there are several exemptions. For instance, the FTC Act exempts common carriers,

nonprofits, and financial institutions such as banks, savings and loan institutions, and federal credit unions.

Consumer Financial Protection Act (CFPA): Similar to the FTC Act, the CFPA prohibits covered entities from engaging in certain unfair, deceptive, or abusive acts. Enacted in 2010 as Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the CFPA created the Consumer Financial Protection Bureau (CFPB) as an independent agency within the Federal Reserve System. The Act gives the CFPB certain "organic" authorities, including the authority to take any action to prevent any "covered person" from "committing or engaging in an unfair, deceptive, or abusive act or practice" (UDAAP) in connection with offering or providing a "consumer financial product or service."

State laws, such as California Consumer Privacy Act (CCPA), and international laws, such as European Union's General Data Protection Regulations (GDPR), aim to provide a comprehensive guidance on digital privacy.[42]

The FTC Act and the Clayton Act are the primary statutes that give the FTC investigative, law enforcement, and litigating authority to protect consumers and promote competition (i.e., antitrust).[43] The FTC "has enforcement or administrative responsibilities under more than 70 laws."[44] The FTC's consumer protection mission currently focuses more on data security issues—such as identity theft, violation of Do Not Call or Do Not Track, and deceptive advertising—than digital privacy concerns associated with lawful activities.[45] While consumer protection and digital privacy are increasingly becoming synonymous, consumer protection law alone may not provide sufficient jurisdiction and authority to encompass digital privacy and data security issues for all data on all devices.

Data Privacy and Data Security

Digital privacy discussions often involve two closely associated topics: data privacy and data security. Data privacy is the governing of data collection, use, and sharing. Data security is protection of data from unauthorized or malicious actors. These two topics often differ in the lawfulness of activities, the intended use of data, and the effect on an individual.

[42] Additional information on foreign government policies, such as EU's GDPR and China's Security First can be found in CRS Report R45584, *Data Flows, Online Privacy, and Trade Policy*, by Rachel F. Fefer.

[43] Federal Trade Commission, "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority," June 7, 2013, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

The Clayton Act (15 U.S.C. 12 et seq.), which was enacted on October 15, 2914, comprises the U.S. antitrust law along with the FTC Act (15 U.S.C. 41 et seq.) and the Sherman Act (15 U.S.C 1 et seq.). According to the FTC, "the Commission is charged under Sections 3, 7 and 8 of this Act with preventing and eliminating unlawful tying contracts, corporate mergers and acquisitions, and interlocking directorates. This Act was amended by the Robinson-Patman Act, Pub. L. No. 74-692, 49 Stat. 1526, codified at 15 U.S.C. §§ 13, 13b, and 21a, under which the Commission is authorized to prevent certain practices involving discriminatory pricing and product promotion. The Hart-Scott-Rodino Act (HSR), adding Section 7A of the Clayton Act, is listed separately." This information is available at https://www.ftc.gov/enforcement/statutes/clayton-act and at http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section12&edition=prelim.

[44] Federal Trade Commission, "Statutes Enforced or Administered by the Commission," https://www.ftc.gov/enforcement/statutes; "What We Do," June 7, 2013, https://www.ftc.gov/about-ftc/what-we-do.

[45] Additional information on Do Not Call or Do Not Track can be found in CRS Report R45070, *Protecting Consumers and Businesses from Fraudulent Robocalls*, by Patricia Moloney Figliola.

Federal Trade Commission, "Data and Visualizations," October 15, 2018, https://www.ftc.gov/enforcement/data-visualizations.

Data security is an aspect of cybersecurity more so than privacy. Data security defends against illicit activities such as theft of data. Data security practices include proactive measures against cyber-attacks and responsive measures such as sending notifications to affected individuals upon a data breach.

Data security issues typically involve actors whose intents are malicious, who carry out unlawful activities, and use data in ways that harm an individual. Examples include breaking into a database or sending spear phishing emails to steal identity and financial information.[46] Stolen identity and financial information are often exploited, causing financial damage to individuals and businesses. Privacy implications arise when personal information is compromised during a data security incident.

Data privacy practices determine how and to what extent data are collected, used, and with whom the data are shared. Data privacy sets the scope for control of personal information—this may include data ownership and responsibilities of involved entities.[47]

Data privacy issues typically arise from lawful activities, but personal information may have been collected, used, or shared beyond given permission or awareness of an individual. The process or results may reveal aspects of an individual that were unexpected. Examples of data privacy issues include mobile apps and websites collecting and using an individual's online activity and location data to suggest targeted ads. In general, such activities are a lawful commercial marketing strategy, from which the customers may benefit in forms of enhanced user experience and discounts. But, these activities become an issue when they lack transparency (i.e., when customers are not aware of what information is collected on them, who shares the information with whom, and how the information is used and for what purpose). Individuals may experience that their rights to privacy have been violated when aggregation of information reveals highly targeted information that an individual did not anticipate.

Key aspects of data privacy—such as data collection, storage, sharing, access, and use—are not defined for digital data that are often leveraged by convergent technologies. These key aspects are defined only for certain types of information, such as medical and financial, where federal laws are in place. Similar guidance is limited or not available for other personal data, such as the following:

- Geolocation data[48] collected by apps;
- Contact information and other user-generated content on social media;
- Video recordings made by smart home IoT devices;
- Voice recordings made by virtual assistants; and
- Vitals and health data collected by fitness tracking wearable IoT devices.

Committees in both the House and the Senate of the 115th Congress held several hearings where technology companies were present as witnesses. Over a dozen bills were introduced in the 115th Congress to address various aspects of data privacy and security; but, none became a law.

[46] Phishing refers to general attempts by malicious actors to deceive victims to steal sensitive personal information such as credit card or financial information, passwords, and account credentials. Spear phishing is a targeted attempt aimed to steal sensitive information from a specific individual. In spear phishing, malicious actors often impersonate a trustworthy entity of a targeted victim.

[47] Y.H. Wong and Humphry Hung, "Information Transparency and Digital Privacy Protection: Are They Mutually Exclusive in the Provision of E-services?," *Journal of Services Marketing* 23, no. 3 (May 22, 2009), pp. 154–164, https://doi.org/10.1108/08876040910955161.

[48] An example of geolocation data is Global Positioning System (GPS) coordinates, where the information can identify the physical location an object including an electronic device.

Committees in both the House and the Senate of the 116th Congress have already held multiple hearings on privacy. Several bills were introduced by the 116th Congress to address data privacy concerns as they relate to technological convergence. These bills include the following:

- H.R. 1282 (Representative Bobby Rush), introduced on February 14, 2019, as the Data Accountability and Trust Act, would "require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information…." This bill would define the term personal information; outline special requirements for information brokers; and assign specific responsibilities to the FTC to regulate commercial entities' data security policies and procedures for using and protecting personal information.
- S. 142 (Senator Marco Rubio), introduced on January 16, 2019, as the American Data Dissemination (ADD) Act of 2019, would "impose privacy requirements on providers of internet services similar to the requirement imposed on Federal agencies under the Privacy Act of 1974." This bill would require the FTC to submit recommendations for privacy requirements for internet service providers.
- S. 189 (Senator Amy Klobuchar), introduced on January 17, 2019, as the Social Media Privacy Protection and Consumer Rights Act of 2019, would "protect the privacy of users of social media and other online platforms." This bill would require commercial entities with an online platform to clearly disclose their practices for personal data collection and use prior to obtaining user consents. This bill also outlines enforcement of privacy requirements by the FTC and the attorney general of each state.
- S. 583 (Senator Catherine Cortez Masto), introduced on February 27, 2019, as the Digital Accountability and Transparency to Advance (DATA) Privacy Act, would provide "digital accountability and transparency." This bill would require commercial entities to clearly disclose its privacy practices for various collected data. This bill also would require the FTC to enforce privacy practices to ensure that the minimum requirements are satisfied.

Data Brokers

According to the FTC, data brokers are

> companies that collect consumers' personal information and resell or share that information with others. Data brokers collect personal information about consumers from a wide range of sources and provide it for a variety of purposes, including verifying an individual's identity, marking products, and detecting fraud. Because these companies generally never interact with consumers, consumers are often unaware of their existence, much less the variety of practices in which they engage.[49]

The FTC classifies data brokers into three categories:[50]

[49] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," May 2014, http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[50] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," March 1, 2012, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

1. Entities subject to the FCRA;
2. Entities that maintain data for marketing purposes; and
3. Non-FCRA covered entities that maintain data for non-marketing purposes that fall outside of the FCRA.

The FCRA governs the activities of credit reporting agencies, such as Equifax, Experian, and TransUnion; entities furnishing information to credit reporting agencies; and individuals who use credit reports issued by credit reporting agencies.[51] These entities subjected to the FCRA fall within the first of the three categories of data brokers listed above. However, the FCRA does not have privacy or data security provisions.

Regarding the second and third categories of data brokers, the FTC report notes that "while the FCRA addresses a number of critical transparency issues associated with companies that sell data for credit, employment, and insurance purposes, data brokers within the other two categories remain opaque."[52] Data brokerage companies include Acxiom, Cambridge Analytica, Corelogic, Datalogix, Epsilon, Exactis, ID Analytics, Intelius, PeekYou, Rapleaf, and Recorded Future in addition to the "big three" credit reporting agencies (Equifax, Experian, and TransUnion).[53]

Many data brokers, which are conducting lawful activities, are self-regulated. As depicted in **Figure 3**, data brokerage companies purchase and aggregate information from various sources, which are also self-regulated. These sources include app developers, websites, and social media.[54]

[51] CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh.

[52] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," May 2014, http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

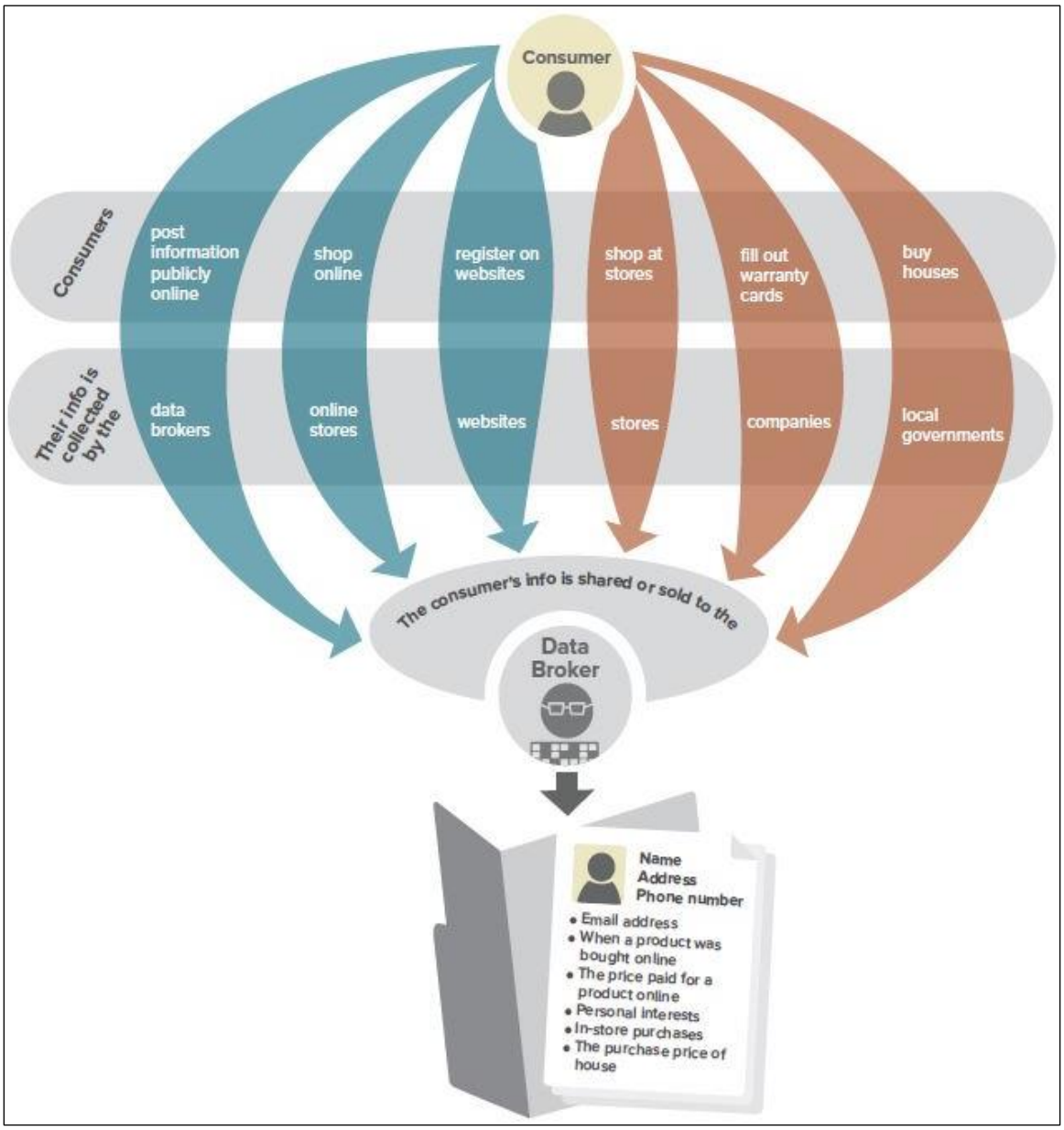
[53] Privacy Rights Clearinghouse, "Data Brokers," https://www.privacyrights.org/data-brokers.

[54] Jennifer Valentino-DeVries et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *New York Times*, December 10, 2018, sec. Business, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Joseph Cox and Jason Koebler, "I Gave a Bounty Hunter $300. Then He Located Our Phone," *Motherboard* (blog), January 8, 2019, https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

Figure 3. Data Collection Online and Offline

As consumers go about their business, data brokers may collect information about them



Source: Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," May 2014, http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

As technological convergence continues to proliferate, more data will likely be generated and consumed. Aggregations of seemingly simple and benign pieces of data when examined together could expose highly personal aspects in detail. Data brokers and entities that collect data could significantly impact digital privacy especially if individuals remain unaware of activities pertaining to their personal data.

Data Security Issues

Congress may be interested in data and physical security aspects of converged technologies because ubiquitous access equates to more possible entry points for both authorized and unauthorized users. This is often referred to as increase in attack surface. As more converged devices become connected to each other and to the internet, the overall impact of a compromise increases, along with the possibility of a cascading effect of a cyberattack. In policies, the requirements and responsibilities of data protection may be addressed separately from privacy concerns associated with legal use of personal data.

Data security, a component of cybersecurity, protects data from unauthorized access and use. Along with digital privacy, data security is a pertinent issue to technological convergence, which generates and consumes large volumes of data. Technological convergence poses a number of different types of potential data security concerns, including the following: potentially increased number of access points susceptible to cyberattacks, linkage to physical security, and theft of data.

Increased connectivity generally translates to increased risk of cyberattack.[55] Converged technologies, such as IoT devices, offer the users ubiquitous access: access from anywhere, at any time, using any device. While this is an extremely convenient characteristic, it also poses cybersecurity concerns. Multiple access points equate to increased points or opportunities for potential exploitation by malicious actors. This is often described as increased attack vectors, or broadening attack surface, which is a sum of attack vectors.[56] The same entry points a user may use for remote access can be exploited by an adversary to steal personal information. From the data security perspective, this is a tradeoff to consider between convenience and vulnerability.

Cybersecurity and physical security are directly linked through converged technologies. For example, when smart doors and smart locks are remotely controlled by a malicious actor through cyberattack, the physical security of that building also becomes compromised. The damage may not be limited to loss of digital content or information. Loss of personal data stored in the compromised location as well as personal security could be in jeopardy.

Potential loss or theft of personal data may be a data security concern for converged technologies because IoT devices often do not employ strong encryption at the device or user interface level. Not implementing strong encryption may be intentional due to associated benefits—it usually keeps the cost low, increases battery life of devices, minimizes memory requirements, reduces device size, and is easier to use or implement. This means, not only is the attack vector increased, but a system is also easier to break into. IoT devices may be the most vulnerable points of a system targeted by malicious actors for exploitation. Some experts note that IoT security currently lacks critical elements such as end-to-end security solutions, common security standards across the IoT industry, and customers' willingness to pay additional cost for enhanced security.[57]

[55] Dan Timpson, "The Internet of Things Is Becoming the Internet of Threats," *Forbes*, https://www.forbes.com/sites/forbestechcouncil/2018/10/24/the-internet-of-things-is-becoming-the-internet-of-threats/.

[56] Pratyusa K. Manadhata, "An Attack Surface Metric" (School of Computer Science, Carnegie Mellon University, 2008), http://reports-archive.adm.cs.cmu.edu/anon/2008/CMU-CS-08-152.pdf.

[57] Harald Bauer, Ondrej Burkacky, and Christian Knochenhauer, "Security in the Internet of Things," McKinsey and Company, https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things.

Congressional Considerations for Technological Convergence

With relatively few policies in place for specifically overseeing technological convergence, Congress may consider potential policy options to address the issues discussed in this report. The fundamental policy considerations to identifying options may be determining the role, if any, of the federal government in overseeing technological convergence, digital privacy, and data security.

Regulatory Considerations

Regulating technological convergence may entail policies for jurisdictional deconfliction, harmonization, and expansion to address blended or new categories of technology. Currently, aspects of converged technologies may be regulated by different agencies based on the individual technologies that compose the convergence, but not as a whole. Regulating a converged technology as a whole can also be challenging because the combinations of technologies may generate too many possible outcomes. When converged technologies establish a new domain and fall outside of existing regulatory jurisdictions, they are often left to self-regulate.

Congress and the Administration could take a number of approaches in regulating technological convergence. Three potential approaches are discussed here. First, the federal government could continue to allow industry to self-regulate, especially where technology evolves quickly. This may promote innovative space, but relies on the industry to exercise responsible and accountable practices.

Second, Congress and the Administration could maintain current regulatory jurisdiction but leverage a deconfliction or harmonization policy so that convergent technologies are regulated under one primary authority instead of potentially multiple authorities. Preserving existing regulatory jurisdiction may require minimal restructuring and allow relatively short timeline for implementation. While a deconfliction or harmonization policy could increase coordination, overlaying such policy on an existing regulatory framework may not present the most efficient process.

Third, the Administration could consider expanding regulatory jurisdictions and authorities to include new and emerging convergent technologies that are self-regulated. This may require a complete overhaul of the technology regulatory framework, requiring congressional action and a relatively lengthy adaptation timeline for the affected industries. Some could also view such actions as extensive regulation that stifles innovation and commercial growth. On the other hand, this approach could present an opportunity to update policies on par with technology progressions and posture for emerging capabilities.

Digital Privacy Considerations

Federal data protection laws currently in place apply to specific types of data and have varied privacy and data security provisions. A federal law that comprehensively addresses digital privacy for all types of data is not in place. While illegal use of personal information (such as identity theft and fraud) is defined and enforced by federal agencies, legal use of data generated by users or converged technologies (such as social media and IoT) is not regulated to the same extent. Transparency into the activities of legal data brokers and collectors is limited.

Congress may choose to define the role of the federal government overseeing digital privacy by introducing new comprehensive federal law(s) and/or by determining minimal required standards of digital privacy. An alternative option could be expanding existing digital privacy authorities. This could include deciding whether federal entities, such as the FTC, should have their rulemaking abilities clarified or expanded.

An expanded or new federal digital privacy policy may require a variety of decisions by Congress. Two of many potential decisions pertaining to federal digital privacy policy are determining how data privacy and data security could be addressed legislatively and determining whether various types, or categories, of personal data should be treated equally or differently under varied guidance.

Data Security Considerations

Data security, as it pertains to technological convergence, may impact both the cyber and physical fronts. Some of the federal data protection laws currently in place have data security provisions, though they vary and may be focused predominantly on the cyber-aspect. This also means that different data security protocols apply to different types of data. For instance, the guidance for notifying users when personal data gets compromised is different for health, financial, and location data.

Similar to the digital privacy considerations, Congress could begin by determining whether overarching legislation for data security is necessary. Congress may consider new legislation explicitly addressing data security concerns pertaining to technological convergence. Or, Congress may consider new legislation to expand existing cybersecurity missions to address data security issues. Data security is often considered as a component of cybersecurity, but protection of the data is equally important as safeguarding a network or a system.

As with any security challenge, finding the right balance between convenience and security measures is a key component of an effective security policy. A data security policy that predominantly focuses on security measures to address potential vulnerabilities created by converged technologies could negate convenient features and beneficial capabilities, such as ubiquitous access, offered by the converged technologies. On the other hand, allowing maximum accessibility without a security measure exposes both the data and the system to risks. Not having an updated data security policy relies on existing cybersecurity measures to address potential vulnerabilities introduced by technological convergence.

Congress may determine whether data privacy and data security should be addressed in one policy. Data privacy and data security are linked and complementary, especially for digital information. While two coupled topics could be addressed in a single policy, data privacy and data security are two distinct issues. Having separate complementary policies could potentially focus more clearly on specific aspects of each issue.

Author Information

Suzy E. Park
Analyst in Science and Technology Policy

Disclaimer