



General Electric Company

Renard Francois
Global Chief Privacy Officer

33-41 Farnsworth Street
Suite 2.D.10F
Boston, MA 02210

T +1 617 443 3432
F +1 202 637-4299

renard.francois@ge.com

November 9, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., N.W.
Room 4725, Attn.: Privacy RFC
Washington, D.C. 20230

VIA ELECTRONIC DELIVERY

Re: NTIA Request for Public Comments on Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01

The General Electric Company (GE) is pleased to respond to the request for public comments concerning "Developing the Administration's Approach to Consumer Privacy." For 126 years, GE has been an engine of progress and economic growth, with more than 100,000 employees in the United States and operations in 170 countries. Today, GE is harnessing the benefits of the Industrial Internet of Things across its full range of businesses, from aviation to energy.

Economic Importance of Industrial Internet of Things (IIoT)

New jet engines carry sensors monitoring everything from pressures and temperatures to vibrations, allowing analysts to spot problems early. Electricity suppliers can use advanced digital technologies to adapt and fine-tune the performance of steam and gas turbines over a lifetime of operation. Wind farm operators use software to extract more power from their existing wind turbines simply by making their machines smarter. Railroads use software to reduce fuel use by and emissions from freight locomotives without turning a single wrench. These early examples are just a glimpse of the promise of future innovation, as more machines generate more data to provide more opportunities to improve the performance, efficiency, and safety of industrial infrastructure.

As the U.S. Federal Trade Commission (FTC) noted in a [2015 staff report](#), the Internet of Things (IoT) encompasses an exceptionally broad range of devices and use cases, from consumer-facing devices to automated communications between machines. The [Center for Democracy and Technology \(CDT\) notes](#) that "what all definitions of IoT have in common is that they focus on how computers, sensors, and objects interact with one another and process data." Cisco has estimated that 50 billion devices will be connected to the Internet by 2020, vastly outnumbering the world's population of human beings. While there are a wide variety of IoT devices and services aimed at home and consumer use, GE's focus is on IoT in the industrial context, i.e., the Industrial Internet of Things, or what GE calls simply the Industrial Internet.

The Industrial Internet refers to the integration of physical machinery with networked sensors and software. The Industrial Internet gathers data from machines, analyzes it in real-time, and then uses it to detect flaws and reduce unplanned downtime. This combination of instrumented devices, the curation and processing of vast quantities of sensor data, and, finally, predictive analytics can have a profound impact on not only industrial processes but also safety, health, energy efficiency, and the

lifespan of industrial assets. The development and deployment of Industrial Internet solutions is accelerating, benefitting our industrial customers, the consumers they serve, and the global economy. This acceleration is driven by multiple factors: new capabilities in software platforms, better network infrastructure, the availability of low-cost storage, cloud computing, and greater “edge” computing capabilities built close to instrumented hardware.

In a [2012 report](#), GE’s chief economist and his co-author found that, in the United States alone, the Industrial Internet could boost average incomes by more than 20% over the next 20 years and lift economic growth back to levels not seen since the late 1990s. If the rest of the world achieved only half of the projected U.S. productivity gains, the Industrial Internet could add more than \$10 trillion to global GDP over the same period. “With better health outcomes at lower cost, substantial savings in fuel and energy, and better performing and longer-lived physical assets, the Industrial Internet will deliver new efficiency gains, accelerating productivity growth the way that the Industrial Revolution and the Internet Revolution did,” the authors wrote.

Within a decade, the economic value of the Industrial Internet will greatly exceed that of the consumer Internet. [In a recent report, McKinsey estimates](#) that the Internet of Things could create a total value of up to \$11.1 trillion on an annual basis by 2025, and that about 70% of this would be captured by business-to-business solutions—leaving the value of the consumer Internet at about \$3.5 trillion.

The Industrial Internet reached an important milestone with the founding of the Industrial Internet Consortium in 2014, charged by its members with promoting initiatives to connect and integrate objects with people, processes, and data using common architectures, interoperability, and open standards. Other trade groups operating in parts of the Industrial Internet space include the Open Connectivity Foundation (encompassing the former Open Interconnect Consortium and AllSeen Alliance) and the OpenFog Consortium.

Various governments also have established efforts to catalyze the digital industrial space, such as Germany’s *Plattform Industrie 4.0*, Smart Factory in the Netherlands, *Usine du Futur* in France, High Value Manufacturing Catapult in the UK, *Fabbrica del Futuro* in Italy, and Made in China 2025 in China. The European Commission has also put forward a policy package on “[Digitising European Industry](#)” as part of the Digital Single Market initiative.

In short, the Industrial Internet is moving quickly, and marked by strong private-sector-led innovation aimed at promoting interoperability for the benefit of industrial customers.

Privacy Considerations Around IIoT

Regarding the Industrial Internet, consumers generally do not interact directly with Industrial Internet devices. Most of the data collected from connected locomotives, turbines, airplane engines, and oil wells concerns the function of the machine itself. Certainly improvements in those machines will have dramatic positive impact for individuals, but these technologies generally do not collect information about consumers.

Most providers of Industrial Internet equipment similarly do not interact directly with consumers. Freight locomotives are sold to railroads and ports, for example. Similarly, utility customers provide energy management solutions to their consumers, relying upon equipment provided by an Industrial Internet provider that may provide analytics concerning grid management and energy efficiency to the utility.

Perhaps most critically, Industrial Internet devices and systems generally do not collect consumer data for purposes of evaluating or marketing/selling to consumers. To the extent personal information is

collected from Industrial Internet systems, it is most often first anonymized or pseudonymized. The data are then used to improve machine and fleet efficiency, increase safety, and to secure networks for the benefit of the consumer, but not for deciding whether to market specific products or services to a particular consumer.

Operators of industrial equipment, such as jet engines or power plants, may correlate data gleaned from IIoT sensors with information about the human operators of the industrial equipment to deliver enhanced insights to the human operators about how they can operate the equipment more safely or efficiently. However, these human operators of equipment are usually employees of the company owning or leasing the equipment, as opposed to consumers. These employees' expectations of privacy in the industrial workplace are different from those of ordinary consumers.

Understanding the distinctions between the IIoT and consumer Internet data and use cases is important in avoiding the misapplication of the same laws used to protect consumer privacy in the case of the Industrial Internet. For example, applying privacy requirements to machine-to-machine communications in the Industrial Internet environment is neither feasible without significant cost and effort, nor would it improve consumer privacy protection. Governments should not impose policies crafted with regard to one sector—for example, the consumer IoT space—upon the Industrial Internet of Things.

Freedom of Contract and IIoT

Industrial Internet services are, by definition, non-consumer, i.e., business-to-business (B2B) or business-to-government (B2G), with legally sophisticated parties on both sides. Contracts are an increasingly common and appropriate mechanism to manage issues such as liability, data rights, customer entitlement to software updates, and intellectual property.

It is also worth noting that the use of contracts is common in the software and Internet space, and has been for decades. There is [well-established case law in the United States and other jurisdictions](#) about the enforceability of license contracts for software. The use of contracts to govern the use of Industrial Internet applications and services builds on this legacy. Government policy should respect and promote freedom of contract.

Recommendations

GE notes that the NTIA RFC appears appropriately focused on consumer privacy as opposed to data used in IIoT contexts. GE applauds the Administration's approach to consumer privacy issues, building on the Fair Information Practice Principles (FIPPS) and the FTC's effective legacy of privacy enforcement actions. Although not the subject of this RFC, GE also is grateful for the Commerce Department's vigorous support for the APEC Cross-Border Privacy Rules (CBPR), which GE believes are crucial in establishing interoperability and mutual recognition of legal regimes to enable IIoT data to flow across borders. GE also lauds USTR's and the Administration's effort to set a high standard on digital trade and data flows in the recently concluded United States-Mexico-Canada Agreement (USMCA).

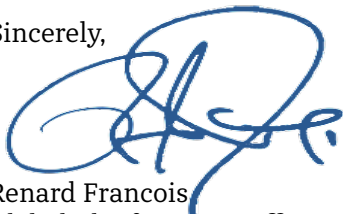
Regarding Administration policy on consumer privacy, GE recommends the following:

- Given the economic importance and potential of IIoT, and the non-personal nature of data generated by sensors on industrial machines, the Administration should recognize that IIoT data, whether raw or aggregated, are fundamentally different from data about natural persons.
- IIoT data should not be included in the scope of whatever legislation or voluntary privacy principles that the Administration might propose.

- In the B2B or B2G context, contracts provide an ideal vehicle for the parties to settle questions of ownership of raw data, insights gleaned from the data, and related use rights. To the extent the Administration's privacy work veers into the B2B IIoT space, which GE would not recommend, freedom of contract should be promoted as an alternative to government-mandated default rules on data ownership, etc.

GE looks forward to the opportunity to engage with NTIA and the Administration as it works both to promote innovation and consumer privacy protection. Thank you for the opportunity to provide our perspectives.

Sincerely,

A handwritten signature in blue ink, appearing to read 'R. Francois', written over a faint circular stamp or watermark.

Renard Francois
Global Chief Privacy Officer
General Electric Company