Smart Factories: Issues of Information Governance

Manufacturing Policy Initiative
School of Public and Environmental Affairs
Indiana University

March 2019

Made possible with support from
Grant Thornton

In collaboration with
MAPI

©asharkyu used under license from Shutterstock®

About the Manufacturing Policy Initiative

Housed within the top-ranked School of Public and Environmental Affairs (SPEA) at Indiana University, the Manufacturing Policy Initiative (MPI) is focused on U.S. public policies impacting the competitiveness of the manufacturing sector. It serves as a source of objective, state-of-the-art information for policy makers, manufacturers, and policy analysts.

The research, outreach, and educational activities of MPI cover the intersection of technology, business, and public policy. The impact of laws and regulations on innovation is a major theme. Three significant conferences/ meetings have been sponsored, including a highly attended September 2016 event outlining a 100-day agenda for the next President of the United States.

For more information, contact Keith Belton at kebelton@iu.edu, or go to: https://manufacturing policy.indiana.edu.

Table of Contents

Executive Summary

To be a successful manufacturer in today's hyper-competitive global marketplace requires relentless innovation to achieve ever-higher levels of productivity.

Nowhere is this more apparent than in smart manufacturing—defined as "the integration of sensors, controls, and software platforms to optimize performance at the production unit, plant, and supply chain levels." Such integration, facilitated by the Industrial Internet of Things (IIoT), allows for real-time decision making via data analytics, including the use of artificial intelligence (AI) techniques, such as machine learning.

Smart manufacturing depends critically on information governance: rules (formal and informal) concerning the collection, flow, and analysis of information, often in digital form. These rules are determined over time through collective action by governmental and nongovernmental organizations. Get the rules right, and the promise of smart manufacturing will eventually become a reality. Get the rules wrong, and smart manufacturing will never fully materialize. Information governance matters.

To explore information governance issues in some depth, the Manufacturing Policy Initiative at Indiana University hosted an October 19, 2018 roundtable event in Washington, DC, featuring executives from nearly 20 manufacturers, each having a global presence. We invited policy experts in academia to contribute papers on specific topics—AI in manufacturing, technical standards, cybersecurity and privacy, and digital trade—to inform and help spur the facilitated discussion. The papers and the discussion—collected in this publication—reveal four important findings:

1. Information governance will impact how and when companies invest in smart manufacturing. Technology alone will not create smart factories—the right policies must also be in place to enable these technologies and reduce unnecessary barriers to market entry.
2. Collective action is needed to create the information governance conducive to investment. Much of this collective action is being initiated by manufacturers themselves, working in coordination with service providers. For example, the increasing availability of cybersecurity insurance is driving best practices throughout supply chains to reduce vulnerabilities. But in some policy areas of import, only governmental action will provide the certainty that drives investment. With respect to digital trade policy, for example, rules on cross-border data flows will eventually emerge through new trade agreements and the resolution of digital trade disputes.
3. The U.S. approach to these information governance issues is not as clear as those of other leading manufacturing nations. China's top-down approach (known as "Made in China 2025," and backed by a significant level of

resources) and Germany's coordinated approach (where government, industry, and academia are in lock-step to achieve Industrie 4.0) stand in stark contrast to the USA's market-driven approach—which has its own advantages. Although the U.S. is making some effort to advance innovation policies to encourage the development of new technologies (e.g., the Manufacturing USA institutes), information governance is receiving much less attention. In fact, there is a noticeable lack of coordination among the various federal departments and agencies engaged in these information governance issues.

4. Policy makers must consider the unique features of domestic manufacturers when crafting policy to address issues of information governance. These features include the distinction between information technology (IT) and operations technology (OT) (which has implications for cybersecurity), the complexity of 21st century supply chains (e.g., the need for information flow within and across global value chains), and the capabilities of smaller firms (e.g., to participate in standard setting development and adoption). Public policy must be informed by such considerations or it is unlikely to attain its objectives.

The Promise of Smart Manufacturing

Keith B. Belton and Ryan Olson*

The competitiveness of a nation's manufacturing sector requires a common pool of capabilities—such as skilled labor, robust supply chains, and specialized services—that together constitute what has been labeled the "Industrial Commons."[1] The more robust the Industrial Commons, the stronger the manufacturing base. And when the Industrial Commons is eroded or weakened, it can be difficult or impractical to restore.

Today, the Industrial Commons is changing. The capabilities needed to ensure competitive success today are different from what they were at the turn of the century. And these capabilities are likely to differ in another five years. The reason? Technology and globalization are transforming where and how goods are produced. To be a successful manufacturer in today's hyper-competitive global marketplace requires relentless innovation to achieve ever-higher levels of productivity.

Nowhere is this more apparent than in *smart manufacturing*—defined as "the integration of sensors, controls, and software platforms to optimize performance at the production unit, plant, and supply chain levels."[2] Such integration, facilitated by the Industrial Internet of Things (IIoT), allows for real-time decisionmaking via data analytics, including the use of artificial intelligence (AI) techniques, such as machine learning. According to consulting firm Deloitte, "the smart factory represents a leap forward from more traditional automation to a fully connected and flexible system—one that can use a constant stream of data from connected operations and production systems to learn and adapt to new demands."[3] This leap forward has been described as a new industrial revolution—one based on digitalization of the supply chain—and a worthy successor to the previous revolutions based on steam, mass production, and information technology. In 2013, Germany branded their efforts to guide this "fourth industrial revolution": Industrie 4.0.

The promise of smart manufacturing is based on a wide array of emerging applications. For example, the application of AI in industrial settings has enabled predictive maintenance (e.g., networked sensors can pick up subtle changes in equipment that may indicate impending failure), enhanced quality control (e.g., an aircraft engine manufacturer can inspect turbofan blades in 3-D with micrometer precision), demand-driven production, inventory optimization, reduced energy and material costs, product design (e.g., Airbus has used generative techniques to create aircraft parts that are significantly lighter than those designed by humans), improved safety, and environmental performance.

---

* *Keith B. Belton is the director of the Manufacturing Policy Initiative in the School of Public and Environmental Affairs at Indiana University. Ryan Olson is a graduate student in public administration at Indiana University.*

These applications are just the tip of the iceberg. When value chains are fully linked digitally to smart factories, unique new applications are likely to emerge; the possibilities are seemingly limited only by entrepreneurial imagination.

The breadth and magnitude of the potential economic impact from smart manufacturing is substantial, and manufacturers of all stripes are taking notice, as recent surveys and marketing forecasts indicate:

- In a qualitative study, Deloitte identifies five characteristics of a smart factory: connected, optimized, transparent, proactive, and agile. Benefits can be expected across a range of categories, including asset efficiency, higher quality products, lower cost, and enhanced safety and sustainability.[4]
- According to a 2018 Accenture study involving interviews across the globe, manufacturing executives believe the pressure to innovate has never been higher, and 71% think AI will have a transformative impact by 2020.[5]
- A July 2017 survey of U.S.-based manufacturers conducted by MAPI and PwC found that 38% of manufacturers are now offering IIoT-driven products and services; an additional 48% are currently in the process of developing them.[6]
- According to a 2015 McKinsey Global Institute analysis of more than 150 use cases, the Industrial Internet of Things (IIoT) can be expected to create between $1.2-3.5 trillion in value added in 2025.[7]
- A 2017 Capgemini survey of 1000 executives of large manufacturing companies (>$1B in annual revenue) led to estimates of the economic impact from smart manufacturing ranging between $1.2 billion and $3.7 trillion in global value add by 2025, and between $500 billion to $1.5 trillion by 2022. This represents a 7x increase in overall productivity by 2022. For a typical automotive original equipment manufacturer (OEM), this productivity increase represents a doubling of operating profit.[8]
- A 2016 U.S. Department of Commerce survey of 80 U.S. manufacturers and vendors suggests that smart manufacturing would provide $57 billion dollars in annual cost reductions.[9] This represents an approximate 3.2% reduction in the shop floor cost of production. Enhanced sensing and monitoring, seamless transmission of digital information, and advances in analyzing data—each has the potential to save manufacturers in excess of $10 billion annually.
- A variety of market research firms estimate the global market for smart manufacturing over the next 5-10 years to be in the hundreds of billions of dollars range: “To reach USD $395.2 billion by 2025” (Grand View Research), “$339B by 2028” (Future Market Insights), “$479B by 2023” (Statista), “$205B by 2022” (MarketsandMarkets), and “$595B by 2023” (Orbis Research).

Despite the substantial benefits that smart manufacturing may bring, such results won’t be easy to achieve. Smart manufacturing faces stiff headwinds.

First, robust processes and devices will not spring up overnight; the needed technologies—such as industrial applications of AI—are evolving. Furthermore, the expertise needed to develop, operate, maintain, and utilize these technologies takes time to cultivate and at sufficient scale to meet demand.

Second, investment cycles in the manufacturing sector are extremely long; complete capital replacement does not happen overnight. The emergence of true “smart factories” will likely begin with new, “greenfield” production facilities; existing factories will adopt smart technologies much more slowly—probably over decades.

Third, the smart manufacturing revolution depends critically on *information governance*: rules (formal and informal) concerning the collection, flow, and analysis of information, often in digital form. These rules are determined over time through collective action by governmental and nongovernmental organizations. Get the rules right, and the promise of smart manufacturing will (eventually) become a reality. Get the rules wrong, and smart manufacturing will never fully materialize. Information governance matters.

To explore information governance issues in some depth, the Manufacturing Policy Initiative at Indiana University hosted an October 19th roundtable event in Washington, DC, featuring executives from nearly 20 manufacturers, each having a global presence. We invited policy experts in academia to contribute papers on specific topics—AI in manufacturing, technical standards, cybersecurity and privacy, and digital trade policy—to inform and help spur the facilitated discussion. Our purpose is to spark a conversation among policy makers and manufacturers about fulfilling the promise of smart manufacturing in the United States.

For the full promise of smart manufacturing to be realized, a step-change increase in both quality and efficiency must be obtained through the real-time analysis of massive amounts of information from within a factory and across the supply chain. This will be achieved through the application of AI. In the paper entitled, "Artificial Intelligence and Manufacturing," David Crandall defines AI, traces its history, describes its strengths and weaknesses, and provides examples of its successful application in a manufacturing setting. A key point is that the factory floor represents a promising venue for AI because it is a controlled environment with limited variables.

For the IIoT to flourish, devices up and down the supply chain must be capable of communicating with each other. Interoperability is a must for smart manufacturing, and this requires a common language—standard protocols for communication. Only through the development of global standards can smart manufacturing reach its full potential. In the paper entitled, "Technical Standards for Smart Manufacturing," Angus Low provides an overview of the standards-development process: the major players, the sheer magnitude of activity underway, and the role that national governments are taking by positioning their country as a first mover. A paradox emerges—technology often moves faster than standard setting, yet standard setting is needed to promote technological development. Firms that seek a competitive edge today have to weigh the pros of being an early adopter with the cons of investing in technologies based on standards that may soon become obsolete. This is a value-of-information problem—the longer a firm waits for a stronger signal of emerging standards, the more certain it can be of a positive investment return, but the less likely the firm will lead the new industrial revolution.

Perhaps the most glaring obstacle to the promise of smart manufacturing is the risk of a cyberattack. In the paper entitled "Smart Factories, Dumb Policy?", Scott Shackelford describes a world where a security threat emerges and is then addressed, only to result in a continuous cycle of ever-more insidious attacks that require real-time development of effective countermeasures. Given the severity of the problem, prevention becomes an imperative. Shackelford describes policy proposals and private-sector actions that together create a polycentric governance to protect the cyber "commons." The reader is left with the impression that such polycentric governance is not only inevitable but also necessary for smart manufacturing to flourish. With respect to privacy, Shackelford emphasizes the leadership of the EU with its General Data Protection Regulation (GDPR)—applicable to manufacturers and driving other countries to develop their own policies. Regulatory requirements to ensure privacy will continue to evolve over the next few years.

Smart factories link digital technologies with production processes. The technologies underpinning smart factories (e.g., 3-D printing, IIoT, etc.) will transform trade in manufactured goods. As Susan Aaronson points out in her paper, "The Trade Impact of Smart Factories," this transformation is pushing policymakers to update trade policies and agreements and develop interoperable norms governing data. However, only two trade agreements, CPTPP and NAFTA 2.0—neither of which is yet in effect—include provisions governing cross-border data flows. Nations are not approaching these issues uniformly. Whereas the U.S. policy is to support a free flow of information across borders, the EU is regulating (restricting the use of) certain types of personal data, and other countries (e.g., China) are restricting the flow of information (e.g., through data localization requirements). Trade disputes have and will continue to arise and be decided before digital trade policy evolves enough to give manufacturers greater certainty.

Manufacturers cannot wait for perfect policy to emerge—the journey to smart manufacturing has already begun, and competitiveness considerations demand participation. In the final paper, "Challenges and Opportunities,"

Keith Belton describes the perception of 18 manufacturing executives as they react to these issues from a business perspective. The reader comes away with a sense of urgency and frustration—urgency to lead in smart manufacturing for competitiveness reasons and frustration over a lack of certainty over these information governance issues. Other related issues also emerge—such as the difficulty in acquiring expertise in data analytics and AI—a problem compounded by the current skills gap in U.S. manufacturing.

As one reads through these issue papers, certain themes emerge:

1. Information governance will impact how and when companies invest in smart manufacturing. Technology alone will not create smart factories—the right policies must also be in place to enable these technologies and reduce unnecessary barriers to market entry.
2. Collective action is needed to create governance conducive to investment. Much of this collective action is being initiated by manufacturers themselves, working in coordination with service providers. For example, the increasing availability of cybersecurity insurance is driving best practices throughout supply chains to reduce vulnerabilities. But in some policy areas of import, only governmental action will provide the certainty that drives investment. With respect to digital trade policy, for example, rules on cross-border data flows will eventually emerge through new trade agreements and the resolution of digital trade disputes.
3. The U.S. strategy/approach to these information governance issues is not as clear as those of other leading manufacturing nations. China's top-down approach (known as "Made in China 2025," and backed by a significant level of resources) and Germany's coordinated approach (where government, industry, and academia are in lock-step to achieve Industrie 4.0) stand in stark contrast to the USA's market-driven approach (which admittedly has its own advantages). And although the U.S. is making some effort to advance innovation policies to encourage the development of new technologies (e.g., the Manufacturing USA institutes), information governance is receiving much less attention. In fact, there is a noticeable lack of coordination among the various federal departments and agencies engaged in these information governance issues.
4. Policy makers must consider the unique features of domestic manufacturers when crafting policy to address issues of information governance. These features include the distinction between information technology (IT) and operations technology (OT) (which has implications for cybersecurity), the complexity of 21st century supply chains (e.g., the need for information flow within and across global value chains), and the capabilities of smaller firms (e.g., to participate in standard setting development and adoption). Public policy must be informed by such considerations or it is unlikely to attain its objectives.

Smart Factories: Issues of Information Governance is based on a premise: smart manufacturing requires the right set of policies in order to flourish. The competitiveness of domestic manufacturing is at stake.

Endnotes

[1] See Gary Pisano and Willy Shih, 2012. *Producing Prosperity,* Harvard University Press: Cambridge, MA.

[2] This definition comes from the following source: National Science and Technology Council, 2018. *Strategy for American Leadership in Advanced Manufacturing*, Office of Science and Technology Policy, October.

[3] Deloitte, 2017. *The Smart Factory: Responsive, Adaptive, Connected Manufacturing*. Deloitte University Press.

[4] Deloitte. 2017. *The Smart Factory: Responsive, Adaptive, Connected Manufacturing*. Deloitte University Press,

[5] Accenture. 2018. *Manufacturing the Future: Artificial Intelligence will fuel the next wave of growth for industrial equipment companies*.

[6] PricewaterhouseCoopers (PwC) and the Manufacturers Alliance for Productivity and Innovation (MAPI), 2017. *Monetizing the Industrial Internet of Things*. PwC. July.

[7] McKinsey Global Institute, 2015. *Unlocking the Potential of the Internet of Things*, McKinsey & Company, June.

[8] Capgemini Digital Transformation Institute, 2017. *Smart Factories: How can manufacturers realize the potential of the digital revolution*? Capgemini Consulting.

[9] Anderson, Gary, 2016. Department of Commerce. "The Economic Impact of Technology Infrastructure for Smart Manufacturing," *NIST Economic Analysis Briefs* 4, October.

Artificial Intelligence and Manufacturing

David J. Crandall*

Artificial Intelligence technology is rapidly moving out of the research lab and into products, with the potential to fundamentally transform many facets of business and everyday life. This paper provides a brief overview of AI, including what it is and what it isn't, when it tends to work well, and when it tends to fail. We then specifically review how it could impact the manufacturing sector in particular.

Introduction

After six decades of research, Artificial Intelligence is finally moving out of the lab and into the real world. Computers now out-perform humans on a range of tasks, from everyday games like Chess and Jeopardy [14, 27] to advanced security systems that recognize faces [29] or read lips [11]. Some AI applications are already commonplace—e.g., smartphones that react to voice commands—while others loom large on the horizon—e.g., self-driving vehicles that could forever transform transportation. This excitement has come with hype and many mysteries: Why can AI defeat every human Chessmaster that has ever lived, but a state-of-the-art AI-powered mall security robot can clumsily drown itself in a fountain because it didn't see it [15]?

What is AI?

Artificial Intelligence is surprisingly difficult: Dr. Herbert Simon, Nobel and Turing Prize laureate, is reported to have predicted in 1960 that "machines will be capable, within 20 years, of doing any work that a man can do" [19]—a goal that is still elusive some 60 years later. The original dream of AI was to replicate the *way that humans think*, so early AI researchers wrote programs that encoded rules for carrying out tasks and making decisions. This turned out to be impractical: even the simplest of everyday activities, like going for a walk around the mall, involves making innumerable choices, observations, and inferences that seem trivial to us but are extremely difficult to express algorithmically. (Even just deciding whether the path ahead is solid remains a challenge, as the aforementioned security robot learned). Today's work in AI aims for the more modest goal of creating systems that can *perform tasks that seem to require human-level intelligence*. Thus modern AI generally tries to reproduce *what* humans can do, not *how* they do it, through a variety of technologies and approaches.

Machine Learning

Instead of writing programs that explicitly instruct a computer how to carry out a task, many AI systems use *machine learning*. Although often described in grandiose terms of replicating humans' abilities to learn, in

* *David J. Crandall is an associate professor in the School of Informatics, Computer Science, and Engineering at Indiana University.*

practice machine learning is simply about *finding patterns in data, and then using those patterns to make predictions about future data*. Consider the simple example of a robot learning to calculate the circumference of a circle from its radius. To do this, it collects "training data" by drawing circles of different radii, measuring the circumferences with a ruler, and then finding a mathematical relationship between the two. Many possible relationships fit the training data, as shown in Figure 1, each making different predictions about unseen data points—some even predict that the circumference can be negative! A human learner might use intuition to choose between them (e.g., discarding models that predict negative circumferences), but algorithms do not have this "common sense." This means that our robot learner may perform very well on its own "training data," but fail spectacularly when it makes predictions about new circles.

Real applications of machine learning involve data that is much more complicated; for face recognition, for example, the data points are not single numbers but images encoded as vectors of millions of numbers. Nevertheless, the basic idea is the same—fitting models to training data. Just like the robot above, machine learning's success is at the mercy of its training data. (This is why face recognition works best on white men [7]: the face training datasets are often of AI researchers themselves, and thus reflect unfortunate biases of STEM demographics.) Ideally, the training set would be large enough to include every possible scenario. In most interesting real-world problems, however, observing all possible scenarios is difficult or impossible: In driving, for example, we *regularly* encounter events that are *individually rare:* a flooded roadway, a child chasing a ball into the street, a mattress flying off of a truck. People make reasonable (if not perfect) decisions even in scenarios they have never encountered before. A major remaining challenge for AI is to build systems that can similarly be trusted to "generalize" beyond the specific training examples that they have seen.

What is the State of the Art?

Despite the limitations, AI is still a powerful tool because it turns out that pattern-finding on vast datasets can solve many problems that seem to require intelligence. For example, in 2016 a computer finally beat a human champion in Go, a board game so complex that it was thought to require human-level intelligence [26,28]. But the algorithm

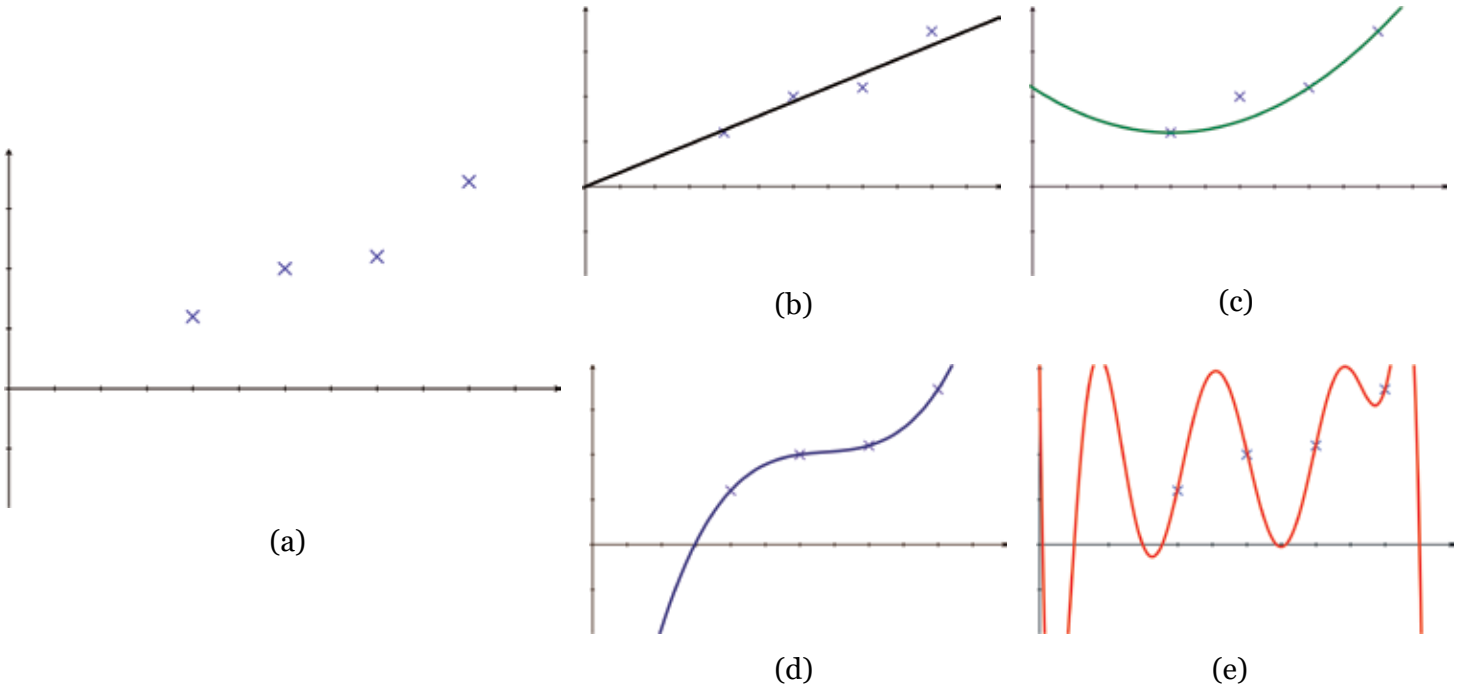

Figure 1. A simple example of the challenges of fitting a mathematical model to observed training data, in order to describe the relationship between two variables (x and y axes). The same four data points in (a) can be fit with numerous possible models of different shapes and complexities, as shown in plots (b) through (e).

solved it in a different way, by playing and finding patterns in nearly 20 million games—many thousands of times more than any human could play. AI's successes are not limited to games, of course. Figure 2 shows examples of AI recognizing specific species of animals in images, from among nearly 3,000 possibilities; its accuracy of about 60 percent, while not perfect, is probably far above that of the average person [30]. Figure 3 shows sample outputs from a system that can answer questions about photos [4, 6, 32], which requires AI to solve multiple problems including understanding a question, recognizing photo content, and producing a correct answer.

These examples all use machine learning, and thus depend on fitting mathematical models in millions of images provided as training data. But because these models are not perfect and do not operate the same way that people do, the results they produce can be perplexing or even nonsensical. The second row of Figure 3, for example,

Figure 2. Sample recognition results from [30], in which the system locates and identifies specific species of animals from among some 3,000 possible classes.

Question: What color is illuminated on the traffic light?

Answer: *red*

What is the man holding?

phone

What color is his tie?

black

What sport is shown?

frisbee

Question: How many oranges are on pedestals?

Answer: *2*

How many zebras?

2

What type of reception is being attended?

cake

What color are the safety cones?

yellow

Figure 3. Sample results of automatic question answering, from [4, 6].

shows visual questions that were incorrectly—and largely inexplicably—answered by the algorithm. Figure 4 shows some examples [20] of pairs of images that look nearly identical but are classified very differently by the computer: just like how some of the circle models would predict negative circumferences despite fitting the training data, the model found here correctly classifies many images but fails on images that are only slightly different. Unfortunately, these misclassifications mean that AI systems can be easily fooled: pranksters could modify the appearance of road signs to make them invisible to autonomous vehicles (Figure 5), for example.

When Does AI Work Well?

Given its imperfections and limitations, deploying AI in the real world must be done carefully. AI works well in applications with very large amounts of high-quality data, and in applications that are resilient to potential errors, typically because (1) a human is "in the loop" to double-check the AI's decisions and intervene if needed, (2) the context or environment is constrained, and/or (3) the consequences of failure are minimal. Board games like Go are perfect for AI because large training datasets are available (the computer can generate many games by just playing against itself), consequences of failure are low, and the environment is constrained by the rules of the game. Autonomous driving, on the other hand, is much more difficult, which explains why many companies are targeting limited scenarios such as requiring a human to have their hands on the wheel to override the system if needed, or working only in controlled scenarios such as Interstate highways.

While computers cannot yet surpass human intelligence, they *can* outperform humans in sheer speed of calculations and ability to search vast amounts of information. They can also be programmed to perform the same task over and over again, impartially and without fatigue. These properties enable new capabilities that would simply not be possible for humans to do alone. For example, AI technology can be used to communicate

Figure 4. Sample adversarial examples from [20]. The first row shows images and the object that the algorithm recognizes. The second row shows the same images corrupted with noise that is nearly imperceptible, but nevertheless causes the classifier to recognize the wrong object.

Figure 5. Graffiti patterns that confuse an autonomous car's sign classification system, causing it to recognize the wrong type of sign, from [12].

with hundreds or even thousands of sensors and other devices at a time, collecting data and making decisions in real-time. Such a network of small devices, or "Internet of Things," can range in scale from dozens of sensors in an automobile, to thousands of sensors in a manufacturing plant, to millions of sensors in consumer products scattered around the world. These sensors can be collecting many different types of information—video, audio, sensor readings, text, etc. Meanwhile, computers' objective and fast calculations let them quickly make quantifications that would not be possible by a human. For example, instead of simply predicting that an important piece of equipment may soon fail based on sensor readings and other data, AI algorithms could predict the *probability* of failure, and compare the expected cost of repairing it once it fails versus the downtime cost of taking it off-line for predictive maintenance.

How Can AI Be Applied in Manufacturing?

Many manufacturing applications are well suited to these advantages of AI. For example:

- **Quality inspection:** In the restricted environment of a manufacturing plant, computer vision can perform many inspection tasks more quickly, accurately, and efficiently than a human. For example, an aircraft engine manufacturer recently began applying computer vision to inspect turbofan blades in 3-D with micrometer precision [9]. The system checks several hundred properties of a blade in just 15 seconds, which has allowed the manufacturer to inspect *every* blade it manufactures instead of just a random sample. Moreover, the system applies a consistent standard, eliminating variations across different human inspectors. Automated inspection may also significantly improve efficiency of consumer product manufacturing: An automated system adopted by a hot sauce maker checks the placement of labels at a rate of over 1,000 per minute [10]. Many of these systems are custom- designed for one particular inspection task and (unlike a human) are unable to be easily retrained. Machine learning-based approaches may change this; machine learning pioneer Andrew Ng recently announced landing.ai, a start-up which promises more flexible inspection systems.
- **Optimizing supply chains:** AI can be used to collect and monitor fine-grained data along the supply chain, and then manage inventory, predict future demand, spot inefficiencies, etc. For example, Walmart is testing indoor drones to monitor its warehouse inventories [3]. It also uses machine learning to forecast product demand based on local weather, for example, and has discovered subtle patterns that may not have occurred to a human forecaster (e.g., that steaks sell better than ground beef when it is cloudy and windy) [21]. The algorithms are not able to explain *why* these patterns occur, or even if they are reliable patterns or simply coincidences, but this is acceptable in this application: the consequences of a few incorrect predictions are minor as long as the system improves efficiency overall. (This is unlike, say, autonomous weapons where explaining why the system chose a particular target would be crucial.)
- **Fine-grained equipment monitoring and predictive maintenance:** AI can monitor manufacturing equipment at a very fine grain through hundreds of networked sensors, picking up on subtle changes—e.g., greater than usual vibration, or slight changes in machine noise—that may indicate impending failure. Mueller Industries, a manufacturer of industrial products, is testing such a system, and already identified a problem with bearings on one of its machines that could have caused significant downtime if it had not been discovered and repaired [8]. This technology has the potential to move from "preventative maintenance" to "predictive maintenance," avoiding machine downtime both from machine failure and unnecessary preventative maintenance.
- **Advanced robotics:** Robots have long been used in manufacturing, but typically must be custom-built for one particular task, cannot be easily "retrained," and are typically blind to their surroundings, simply performing the same task over and over regardless of what (or who) might be in the way. New technology is starting to allow robots to perceive human activities and safely collaborate with them [18]. Other research is investigating robots that can automatically learn by imitating human actions—that could dramatically reduce development costs—or that can learn on their own by simply "practicing" a task over and over again until they succeed [13]. Most of this work is still in the proof-of-concept stage, but the technology is advancing quickly.

- **Generative design:** AI can be used to simulate how a design would perform in the real world, without physically building it, and then automatically "evolve" modifications until an optimal design is reached. As just one example, Airbus reportedly used generative techniques to create aircraft parts that are significantly lighter than those designed by humans [5].
- **Augmenting human capabilities:** Collaborating humans and AI can potentially perform better and more efficiently than either individually. For example, Augmented Reality (AR) can enhance efficiency by showing workers important information as they perform a task, and allowing them to see views that would not otherwise be possible (e.g., infrared imaging to see in low light). One study reported a 34 percent improvement in productivity for a worker performing a wiring task when AR glasses were used to guide the process [2].
- **Transportation:** Autonomous vehicles have the potential to revolutionize the world's transportation systems *eventually*, but numerous technical, social, legal, and ethical problems remain before they will likely see widespread consumer use [17]. But autonomous vehicles in more restricted settings, such as manufacturing floors, are already being deployed. Amazon reportedly uses tens of thousands of robots to automatically move products in its warehouses [25], for example. And autonomous long-haul trucking may arrive much sooner than autonomous consumer vehicles, since navigating the restricted setting of Interstate highways is significantly easier than handling all possible roadways [24]. Semi-autonomous trucks with assistive safety features are already becoming commonplace.

What is the Road Ahead?

Although AI can outdo humans on some very specific tasks, humans still dramatically outperform in practically all real-world tasks requiring intelligence [23]. Moreover, machine learning algorithms require huge training sets, whereas humans can learn with very limited experience. Finally, while humans can offer reasoning to support their conclusions, machine learning is a "black box" that typically cannot explain or defend its answers. It may just be a matter of time before these limitations are solved, or they may be more fundamental. Some believe that human learning is nothing more than a sophisticated version of model fitting [1], while others believe that current AI techniques are inherently "wrong" and could never mimic the complex reasoning that people do [16, 22, 31]. Regardless, AI is advancing rapidly, having achieved milestones that seemed unreachable even a few years ago. Current AI technology can already be usefully applied in many applications, particularly in the manufacturing sector, where data is copious, operating environments are restricted, and trained humans can oversee the automatic systems.

Beyond the technical challenges, AI also raises important legal, ethical, and public policy questions. AI will have to make potentially life-or-death decisions—how should a self-driving car choose between crashing itself and potentially killing its passengers, versus striking a child who has run into the road? To what extent should the algorithms that make such choices be subject to government oversight? How do we assign liability for when AI makes mistakes? How do we safeguard AI systems, to protect both the data they collect and decisions they make from hackers and other adversaries? In general, what protections are needed, if any, to ensure that AI does more good than harm?

References

[1] "Why humans learn faster than AI—for now," *MIT Technology Review*, March 7, 2018.

[2] Magid Abraham and Marco Annunziata, 2017. "Augmented reality is already improving worker performance," *Harvard Business Review*, March 13.

[3] Rachel Abrams, 2016. "Walmart looks to drones to speed distribution," *The New York Times*, June 2.

[4] Aishwarya Agrawal, Dhruv Batra, and Devi Parikh, 2016. "Analyzing the behavior of visual question answering models," *Conference on Empirical Methods in Natural Language Processing (EMNLP)*.

[5] Ravi Akella, 2018. "What generative design is and why it's the future of manufacturing," *New Equipment Digest*, March 16.

[6] Peter Anderson, Xiaodong He, Chris Buehler, Damien Teney, Mark Johnson, Stephen Gould, and Lei Zhang, 2017. "Bottom-up and top-down attention for image captioning and VQA," *arXiv:1707.07998*.

[7] Joy Buolamwini and Timnit Gebru, 2018. "Gender shades: Intersectional accuracy disparities in commercial gender classification," *Conference on Fairness, Accountability and Transparency, FAT 2018*, pages 77–91.

[8] Tim Caldwell, 2017. "Case study: Mueller moves from preventive to predictive maintenance," *Control Design*, April 6.

[9] Jim Camillo, 2015. "Robots and Machine Vision Automate Inspection of Jet Engine Parts," *Assembly Magazine*, September 3.

[10] James Carroll, 2013. "Machine vision system inspects Tabasco hot sauce products," *Vision Systems Design*, October 10

[11] Joon Son Chung, Andrew Senior, Oriol Vinyals, and Andrew Zisserman, 2016. "Lip reading sentences in the wild," *arXiv:1611.05358*.

[12] Ivan Evtimov, Kevin Eykholt, Earlence Fernandes, Tadayoshi Kohno, Bo Li, Atul Prakash, Amir Rahmati, and Dawn Song, 2017. "Robust physical-world attacks on machine learning models," *arXiv preprint arXiv:1707.08945*.

[13] Daniel Faggella, 2017. "Machine learning in robotics – 5 modern applications," *Techemergence.com*, December 5.

[14] David Ferrucci, Eric Brown, Jennifer Chu-Carroll, James Fan, David Gondek, Aditya A. Kalyanpur, Adam Lally, J. William Murdock, Eric Nyberg, John Prager, Nico Schlaefer, and Chris Welty, 2010. "Building watson: An overview of the deepqa project," *AI Magazine*, 31(3).

[15] Natt Garun, 2017. "DC security robot quits job by drowning itself in a fountain," *The Verge*, July 17.

[16] Douglas Hofstadter, 2018. "The shallowness of Google translate," *The Atlantic*, January 30.

[17] Nidhi Kalra and Susan M. Paddock, 2016. "Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?" *Transportation Research Part A: Policy and Practice*, pages 94:182-193.

[18] Will Knight, 2018. "This company tames killer robots," *MIT Technology Review*, June 15.

[19] Raymond Kurzweil, 1985. "What is Artificial Intelligence Anyway?" *American Scientist*, 73(3).

[20] Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, Omar Fawzi, and Pascal Frossard, 2016. "Universal adversarial perturbations," *arXiv preprint arXiv:1610.08401*.

[21] Jack Neff, 2014. "Cloudy with a chance of meatballs: How weather forecast predicts Walmart's sales outlook," *AdAge*, October 27.

[22] Judea Pearl, 2018. "Theoretical impediments to machine learning with seven sparks from the causal revolution," *arXiv:1801.04016*.

[23] P. Jonathon Phillips, Matthew Q. Hill, Jake A. Swindle, and Alice J. O'Toole, 2015. "Human and algorithm performance on the pasc face recognition challenge," *IEEE International Conference on Biometrics Theory, Applications and Systems*.

[24] PwC, 2018. *Industrial mobility: How autonomous vehicles can change manufacturing*.

[25] Sam Shead, 2017. "Amazon now has 45,000 robots in its warehouses," *Business Insider*, January 3.

[26] David Silver, Aja Huang, Chris J Maddison, Arthur Guez, Laurent Sifre, George Van Den Driessche, Julian Schrittwieser, Ioannis Antonoglou, Veda Panneershelvam, Marc Lanctot, et al., 2016. "Mastering the game of go with deep neural networks and tree search,"*Nature*, 529(7587):484-489.

[27] David Silver, Thomas Hubert, Julian Schrittwieser, Ioannis Antonoglou, Matthew Lai, Arthur Guez, Marc Lanctot, Laurent Sifre, Dharshan Kumaran, Thore Graepel, Timothy P. Lillicrap, Karen Simonyan, and Demis Hassabis, 2017. "Mastering Chess and Shogi by self-play with a general reinforcement learning algorithm," *arXiv 1712.01815*.

[28] David Silver, Julian Schrittwieser, Karen Simonyan, Ioannis Antonoglou, Aja Huang, Arthur Guez, Thomas Hubert, Lucas Baker, Matthew Lai, Adrian Bolton, et al., 2017. "Mastering the game of Go without human knowledge," *Nature*, 550(7676):354-359.

[29] Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf, 2014. "Deepface: Closing the gap to human-level performance in face verification," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 1701-1708.

[30] Grant Van Horn, Oisin Mac Aodha, Yang Song, Yin Cui, Chen Sun, Alex Shepard, Hartwig Adam, Pietro Perona, and Serge Belongie, 2018. "The iNaturalist Species Classification and Detection Dataset," *arXiv:1707.06642*.

[31] James Vincent, 2017. " Facebook's head of AI wants us to stop using the Terminator to talk about AI: Yann LeCun chats about super-intelligent AI and the future of virtual assistants," *The Verge*, October 26.

[32] Qi Wu, Peng Wang, Chunhua Shen, Anthony Dick, and Anton van den Hengel, 2016. "Ask me anything: Free-form visual question answering based on knowledge from external sources," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 4622-4630.

Peer Reviewers: Les McHargue, Director, Analytic Services, Grant Thornton, and Wilfred Mascarenhas, Advisor—Data & Analytics, Manufacturing and Quality IT, Eli Lilly and Company.

Technical Standards for Smart Manufacturing: Evolution and Strategic Positioning

Angus Low*

Twenty-first century manufacturing is being transformed rapidly by two forces—globalization and technology. As a result of this transformation, manufacturers face a hypercompetitive environment where information governance is critical to their survival and success. One concept that is receiving great attention is smart manufacturing (SM)—the convergence of operating technologies (OT) and information technologies (IT) working together in a real-time integrated fashion. The promise of SM is considerable: between $500 billion and $1.2 trillion in added value globally within five years.[1] Estimates such as these reflect efficiencies related to preventative maintenance, operations on the factory floor, supply chain management, and logistics.

The pace of SM will depend critically on the development and global adoption of technical standards, which provide uniformity that allows for acceptance and use and therefore encourage trade.

From the perspective of a smart manufacturer, standards facilitate two goals: to enable the integration of technologies using safe and secure methodologies, and to demonstrate compliance with regulations that incorporate standards by reference. Without technical standards, SM would be far more expensive and uncertain.

The SM standards landscape is multifaceted, complex, and ever-evolving. It is also high stakes: First-mover advantages will accrue to those who lead the way in establishing truly global standards. The active role that other national governments are playing to develop SM standards to benefit their domestic manufacturing sector raises certain policy issues that the U.S., as a leading manufacturing nation, cannot ignore.

What is Smart Manufacturing?

Multiple definitions of "smart manufacturing" can be found (e.g., from NIST, the Clean Energy Smart Manufacturing Innovation Institute, etc.). According to Dan Green, Director of the Joint Advanced Manufacturing Region (JAMR) within the Navy, Smart manufacturing is "the convergence of operating technologies (OT) and information technologies (IT) working together in a real-time integrated fashion."[2] In other words, it is the ability for information to be communicated between the manufacturing floor and the enterprise's connected and cloud based information systems automatically and in real time. Other definitions emphasize the integration of technologies (such as IIoT, robotics, additive manufacturing, big data and cloud computing, advanced analytics and AI, and virtual and augmented reality).

---

* *Angus Low is Global Product Standards and Regulation Manager at Rockwell Automation.*

Traditional manufacturing processes have not always included this instant and "live" connection, and therefore the ability of the enterprise, or its customers, to know the status of the whole system has relied on more manual methods of reporting. This traditional approach creates inefficiencies and delays that compromise the ability for enterprises to compete domestically and internationally. SM also adds a data point to the calculation that has hitherto been mostly ignored: people. Many production lines today incorporate robots that work alongside human workers in a safe and secure manor. Ensuring connections between OT and IT while taking into account the human factor has increased complexity, requiring across-the-board standardization to avoid communication conflicts as well as potentially hazardous situations.

The Standards Development Landscape

Standards are documented agreements containing specifications applied consistently as rules or guidelines for materials, products, processes, or services (such as communication between machines, systems, hardware and software, etc.). They provide uniformity that allows for acceptance and use, and therefore benefit manufacturers by limiting barriers and facilitating trade. Seen in this light, standards facilitate innovation.[3]

Defining the global standards landscape is not a simple task because there are numerous ongoing activities shaping and reshaping all aspects of SM. Not only are new and disruptive technologies being invented that are redefining the scope of SM, but national initiatives are being developed that are designed to benefit, or in some cases protect, the industrial base within the country's own borders. To understand the current state of play, it is useful to start by understanding the major players and their activities.

Standards can be developed in different ways. The most traditional is through a standards development organization (SDO), which facilitates consensus and makes the resulting standard available to everyone. SDOs can be international, national, or even professional organizations (e.g., an association) that represent their members' common interests. Standards developed in this traditional way often take years to be published. An open source process is sometimes used to develop a standard outside of the traditional SDO process because it is speedier. Ownership of an open source standard is viewed as a public trust and anyone can participate in the development process, which is usually overseen by an independent organization. Once developed, these open source standards can then be adopted into SDOs and become more widely accepted internationally.

Within the realm of SM standards, numerous organizations are involved, including SDOs, consortia, professional associations or trade associations working within their narrow fields, and academically oriented professional societies. Standards are seldom finalized in their first iteration and typically evolve to keep pace with changing technology and use patterns.

SDOs (for example the International Association of Automation [ISA] and the International Organization for Standardization [ISO]) are relied upon for the development of new technical standards that will enable the technologies without favoring any one group in particular. The International Electrotechnical Commission (IEC) publishes standards and coordinates with other standards development groups to provide structure and identify gaps where new standards may be required. SDOs may have agreements with countries to help prevent the localized development of standards from running out of control and creating barriers to trade.

Consortia tend to focus on integrating standards. Participants in consortia agree to use the standards, prove them in testbeds, and collaborate to resolve issues. Many different consortia are involved in SM standards. Consortia that involve the government, industry, and academia tend to focus on how to best leverage existing standards to fill data gaps rather than develop new standards.

Associations and foundations are heavily involved in standards development, and although more focused on specific technologies that support their market segment, can have far reaching influence on other sectors where

overlaps exist. Organizations such as the OPC Foundation, the Open Process Forum, and ODVA are helping to shape the technologies that will help shape the framework for Smart Manufacturing, as well as identifying the technologies that will enable it.

National governments are also involved in developing SM standards because they realize the value that manufacturing brings to their economy and believe that digitalization will elevate the productivity of their domestic manufacturing base. Each national effort is known by a different name: Germany originated Industrie 4.0, China developed a plan known as Made in China 2025, the U.S. established the Manufacturing USA program, and France has its Industrie de Futur. So far, the goals of these efforts have mostly focused on assembling existing standards and creating new standards to meet the larger system needs, but some have very specific strategies to identify standards that enable their vision for SM.

To facilitate the development of SM standards, models have been developed to map the standards landscape. NIST has developed the SM ecosystem (Figure 1) to illustrate the types of standards needed across a manufacturing value chain. The core of the ecosystem is the pyramid, which is based on the hierarchy within ISA 95 (a common reference model for developing automated interfaces between enterprise and control systems). The base of the pyramid is the device level, then the SCADA (Supervisory Control and Data Automation) level, then the MOM (manufacturing operations management) level, and the top of the pyramid is the enterprise level. Crossing through the pyramid are three dimensions—product, production system, and business—each with their own segments and information flows. Numerous SM standards are needed to support every level of the pyramid, each segment within each dimension, and horizontal and vertical integration across the value chain.

Industrie 4.0 has developed its own model, as shown in Figure 2. This model is built around the life cycle and value stream, hierarchy levels, and layers.

Although each model has a different perspective, they share many similarities such that the resulting list of standards identified by each are very similar. Certain standards are seen as especially important in enabling SM—these serve as the building blocks that apply to different levels and different domains within the manufacturing systems.

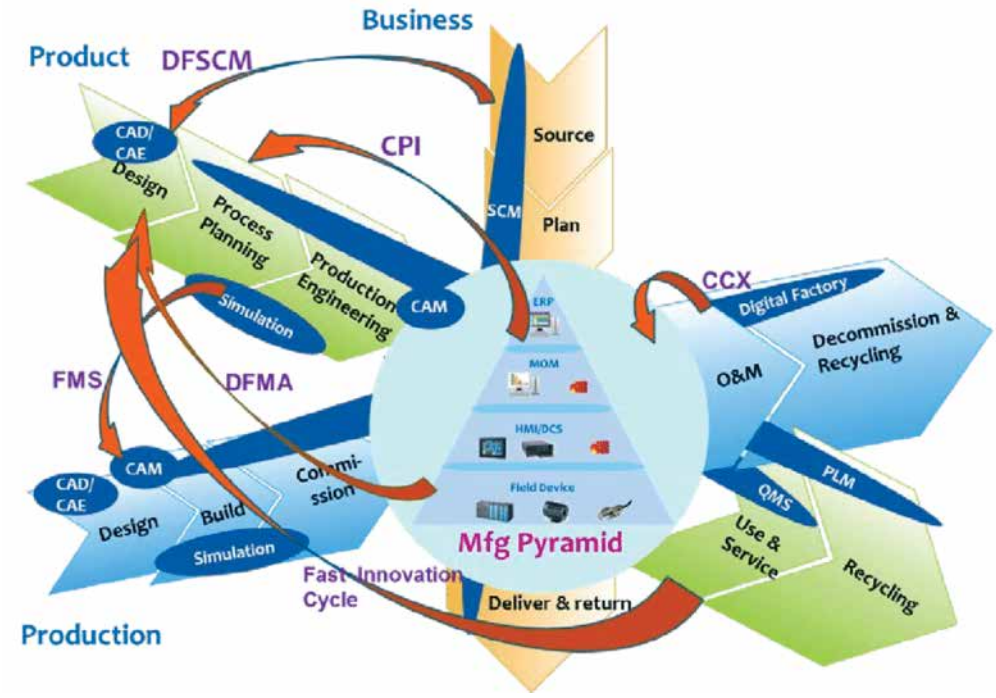

Figure 1. Smart Manufacturing Ecosystem (NIST).

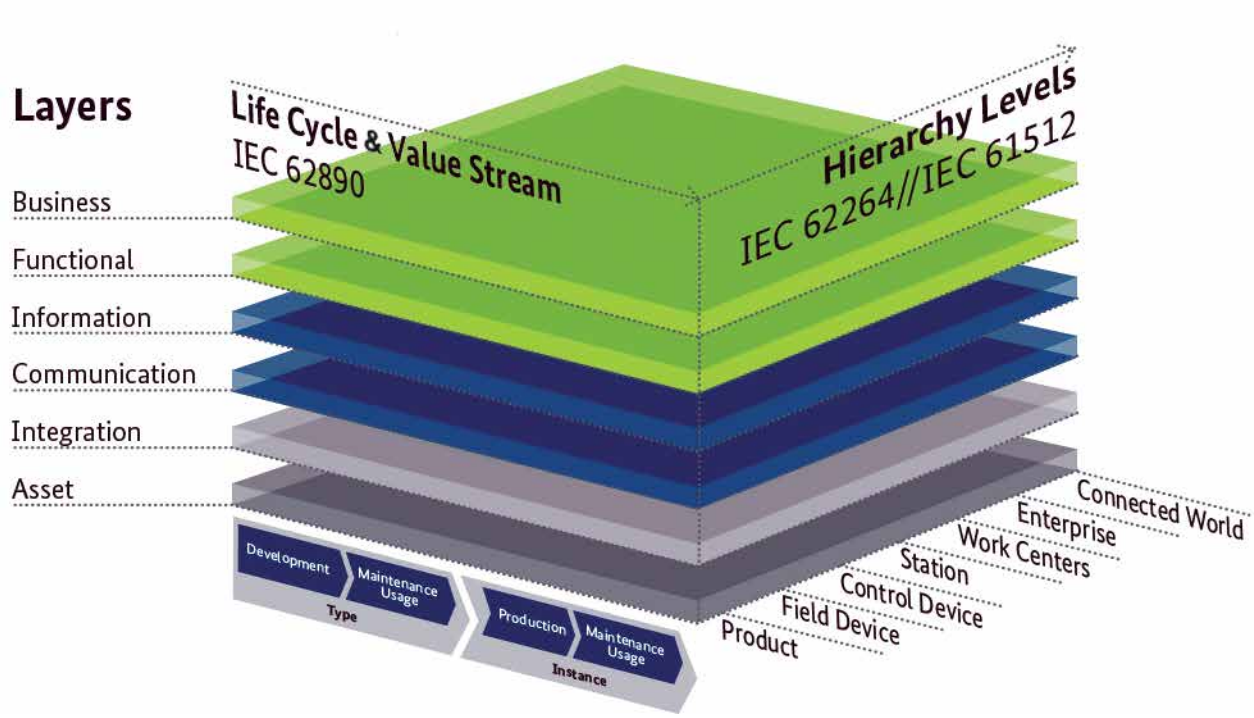

Figure 2. Reference Architecture Model Industrie 4.0.[4]

Challenges for Manufacturers Seeking Standards

Manufacturers who seek to invest in smart manufacturing face significant indirect challenges related to technical standards:

- navigation of the multifaceted standards landscape is complicated by missing, superfluous, and redundant standards;
- the time to develop a standard is lengthened greatly by gamesmanship of the process by various stakeholders; and
- rapidly evolving technology frequently outpaces standards development.

As illustrated by Figure 1, the standards landscape for smart manufacturing—in its most simplified form—is multidimensional, interdependent, and rapidly evolving. The number of standards in existence or under development is in the hundreds if not thousands. Such an intricate landscape is further complicated by missing, superfluous, and redundant standards. According to NIST (2016), gaps in the SM standards landscape include "cybersecurity, cloud-based manufacturing services, supply chain integration, and data analytics." Of the existing standards, a large proportion (at least 25-30 percent) have never been used. SDOs rarely remove a standard once it is developed. Another problem is that existing standards are often identical or nearly equivalent and this raises questions about the most authoritative source. Adding to this confusion is the pluralistic U.S. standards system, where no single entity is authorized to provide standards (e.g., the U.S. has more than 600 SDOs). Because so many standards arise from so many sources, products designed for one market are effectively blocked out of other markets, creating barriers to trade.

The time to develop a standard is lengthened greatly by gamesmanship of the process by various stakeholders. There are some competing efforts around the higher level standards, and who gets to define what the common models are as well as the common sets of underlying standards that adhere to the models. Companies actively involved in standards development in the industrial manufacturing domain seem to be in a constant chess game, analyzing each other's actions and strategies to prevent any one company from including requirements that will

benefit their technology over another. This results in huge expenditures of resources and money that adds to the burden of compliance. IP that is written into standards is a very serious concern as it locks manufacturers into single, proprietary systems that benefit IP owners. This restricts the free development of new technologies or processes and limits organizations from being agile enough to rapidly adapt to disruptive technologies.

Perhaps the most fundamental challenge is that the IT world moves much more quickly than standards development. New IT evolves, on average, every three years, while standards development takes up to five years. IT developers will not wait because by the time the standard is ready and published, they will have moved on to the next version. In addition, IT developers often do not want to get "locked in" to a single vendor's solution based on a standard because it will limit their scope of new technologies. Unlike IT, operational technology (OT) evolves at a slower pace and is less likely to race ahead of standards development.

Given these many challenges, it is not be surprising that competitive pressures may require manufacturers to make investment decisions in the absence of globally adopted standards. As a practical matter, some technologies will be adopted before the needed standards are developed and some projects will employ proprietary standards from vendors. A manufacturer might start with custom integration using proprietary standards from a single vendor, followed by integration using a proprietary standard supported by a group of vendors working as partners, followed by integration using open standards with a myriad of vendors and vendor options.

List of Policy Issues/Questions

From a U.S. perspective, several policy issues/questions arise relating to technical standards for SM:

- Should the U.S. have an overarching strategy for SM standards akin to that of some other countries? If so, what should be the articulated goal?
- Which SM standards or type of SM standards should receive the highest priority of the U.S. government in the near-term (e.g., by 2020) and longer term (e.g., by 2025 and 2030) if the goal is to promote industry investment in SM?
- Should the U.S. government elevate in priority the development of SM standards for the application of AI?

Should the U.S. have an overarching strategy for SM standards akin to that of some other countries? If so, what should be the articulated goal?

In recent years, several countries have adopted policies to digitalize their manufacturing sector. Ezell (2018) summarized these developments across ten countries.[5] Notable among these efforts is Industrie 4.0 (Germany) and Made in China 2025.

Germany is developing technical standards and pushing for their international adoption, starting within the EU. Its management organization, Plattform Industrie 4.0, supported development of the Reference Architectural Model for Industrie 4.0 (RAMI), which is a guide to standards and interoperability. According to published reports, Germany is aggressively pushing development of its standards, which are widely considered "rigorous, comprehensive, and inclusive," according to Ezell. His conclusion: "The risk for Germany is that, while its standards-development process is intensely rigorous, comprehensive, and inclusive, it may take too long, such that by the time the standard is set the technology and market have moved on to something better." In its efforts, Germany is investing heavily in standards adoption (more than the U.S.) and seeking global partnerships.

China's efforts in standardization are government-directed, though it has recently changed its standardization law to encourage association (nonprofit) standards. China has made development of its own standards a linchpin of its economic development strategies, designed to gain a competitive edge over other countries. This is believed

to hold true for its own efforts in standards for digitalizing its manufacturing sector. According to Ezell, "China appears to be playing a short and long game with smart manufacturing standards development; collaborating now where necessary, but in the background developing standards for the future that are designed to give Chinese manufacturers strategic advantage."

The U.S. does not have a formal national strategy with regards to standards and SM other than to facilitate innovation and allow the best solution to emerge, but there are active initiatives from multiple groups and organizations, including government organizations such as the National Institute of Standards and Technology (NIST), SDOs such as Underwriters Laboratories, research institutes such as the Digital Manufacturing and Design Innovation Institute (DMDII)[6] within Manufacturing USA, and individual companies. Ezell described the U.S. posture as favoring "a voluntary, consensus-based, market-driven approach where government agencies participate in the standards development process by being invited to the table . . . but not by overtly directing the process."

At times, the focus on a particular technology or market segment results in a fairly coordinated approach within the U.S., but the lack of a single driving national strategy from which to gain direction for these activities more often than not results in outcomes that are, at best, lackluster. Unless the United States is actively creating, and communicating, a single strategy that helps to advance the manufacturing objectives of domestic companies, it will be very difficult to influence the direction of standards globally, as other countries are doing. In contrast, a national strategy could help align all stakeholders (e.g., NIST, trade associations, industry consortia, etc.) and drive global standards that benefit the manufacturing value chain and bolster the domestic economy.

Which standards or type of standards should receive the highest priority of the U.S. government in the near-term (e.g., by 2020) and longer term (e.g., by 2025 and 2030) if the goal is to promote industry investment in SM?

Whether or not the U.S. government develops a national strategy for SM standards, an important question relates to the appropriate U.S. priorities. In a 2016 report describing the SM standards landscape,[7] NIST listed some of its ongoing activities: "NIST is heavily engaged in efforts to develop new standards for the Digital Thread, Model-Based Enterprise, smart manufacturing design and analysis, additive manufacturing, and robotics. NIST leads an effort to define requirements eventually leading to standards for cloud-based services for manufacturing. NIST work on cybersecurity for supply chains and industrial systems will have great importance for manufacturers. Finally, NIST coordinates the networking of the Manufacturing USA institutes."

Also in that report, NIST listed existing manufacturing standards that are insufficient to enable smart manufacturing: cybersecurity, cloud-based manufacturing services, supply chain integration, and data analytics.

Finally, NIST identified the following priority areas where SM standards are critically needed: SMS reference model and reference architecture, IIoT reference architecture for manufacturing, manufacturing service models, machine-to-machine communication, integration of PLM/MES/ERP/SCM/CRM, cloud manufacturing, manufacturing sustainability, and manufacturing cybersecurity.

Given the large number of standardization efforts underway including those recently initiated, it is not clear that these lists reflect the current standards landscape.

Should the U.S. government elevate in priority the development of SM standards for the application of AI?

Thus far, the standards described in this paper relate to standards for communication and transmission of information across the supply chain in light of the IIoT. But a rapidly emerging area of standards development relates to the real-time analysis of digital information through application of artificial intelligence (AI) techniques.

AI, which is well-suited to manufacturing[8], requires standardization to realize its potential. Machine learning provides one example. "To scale Deep Learning into a practice that is predictable, reliable, and efficient will require standardization. The intent of standardization is to maximize participation of many independent parties. It is a common language or a coordination mechanism for parties to accelerate progress. Accelerated progress is necessary for Deep Learning to not just be confined to research labs but also to be industrialized and available to many."[9]

China plans to be the world leader in AI and in standardization of AI; the country has been moving aggressively to set policies in this regard.[10] For example, China recently released its "Artificial Intelligence Standardization White Paper," developed with help from 30 research institutions, education institutes, and AI companies. This paper includes the following passage: "AI is a prospering new industry. China is at the starting line as all other countries and there is opportunity now for rapid breakthrough. With fast action plans, China can either seize the commanding heights of innovation standardization, or else miss the opportunity. There is an urgent need to seize opportunities, accelerate research on AI deployment in industry, and systematically review and establish a unified and comprehensive set of standardization."[11]

Chinese officials believe the country has a comparative advantage in AI: its sheer size and use of centralized planning allow it to access and utilize massive amounts of data, providing it with training data used in machine learning to develop more efficient algorithms.[12] Given China's plan to elevate innovation in its manufacturing sector (*Made in China* 2025), its focus on AI is hardly surprising.

Conclusion

Given the promise of SM, the critical role of technical standards to realize this promise, and the strategic actions of international stakeholders, now is the time for the U.S. to reflect on its role in the global standards process and make any necessary adjustments. Such reflection should be conducted with input from both domestic and international stakeholders because both national and global action will shape progress. Lack of considered deliberation on this issue will maintain the status quo, where strategic decisions by other countries are likely to shape the competitive landscape for advanced manufacturing for decades to come.

Endnotes

1 Capgemini Consulting, 2017. *Smart Factories: How Can Manufacturers Realize the Potential of Digital Industrial Revolution*.

2 Dan Green, Director of the Joint Advanced Manufacturing Region (JAMR) within the Navy: https://www.nist.gov/blogs/manufacturing-innovation-blog/so-what-exactly-smart-manufacturing.

3 Hui, Liu and Carl F. Cargill, 2017. *Setting Standards for Industry: Comparing the Emerging Chinese Standardization System and the Current U.S. System*, East-West Center: Honolulu, Hawaii.

4 https://www.researchgate.net/figure/Reference-Architecture-Model-Industrie-40-RAMI40_fig1_320916562 (© Plattform Industrie 4.0).

5 Stephen Ezell, 2018. "Why Manufacturing Digitalization Matters and How Countries Are Supporting It," Information Technology and Innovation Foundation (ITIF): Washington, D.C., April.

6 The DMDII is a Chicago consortium led by UI LABS which was the recipient of a $70 million Department of Defense (DOD) grant. matched by $250 million of private sector, academic and local government funding.

7 Yan Lu, K.C. Morris, and Simon Frechette, 2016. *Current Standards Landscape for Smart Manufacturing Systems*. NIST, February.

8 According to Andrew Ng, founder of the deep-learning Google Brain project. See Jean Thilmany, 2018. "Artificial Intelligence Transforms Manufacturing," asme.org, May.

9 Carlos E. Perez, 2018. *Medium*, Why Deep Learning Needs Standards for Industrialization, February 9.

10 In January 2018, *The Asia Times* reported that China believes the timing is right to set industry standards for AI. See *Asia Times*, China aims to lead industry standards, January 11, 2018.

[11] Meghan Han, 2018. *Synced: AI Technology and Industry Review*, "China Aims to Get the Jump on AI Standardization," January 25.

[12] Greg Williams, 2018. *Wired*, "Why China Will Win the Global Battle for AI Dominance," April.

Peer Reviewers: Radu Pavel, Vice President and Chief Technology Officer, TechSolve; Haresh Malkani, Chief Technology Officer, CESMII, University of California-Los Angeles; Jim Davis, Vice Provost, Information Technology, University of California-Los Angeles; Roy Whittenburg, President, MBD360 LLC; and Wilfred Mascarenhas, Advisor—Data & Analytics, Manufacturing and Quality IT, Eli Lilly and Company.

Smart Factories, Dumb Policy? Managing Cybersecurity and Data Privacy Risks in the Industrial Internet of Things

Scott J. Shackelford, JD, Ph.D.*

Ubiquitous computing names the third wave in computing, just now beginning. First were mainframes, each shared by lots of people. Now we are in the personal computing era, person and machine staring uneasily at each other across the desktop. Next comes ubiquitous computing, or the age of calm technology, when technology recedes into the background of our lives.

~ Mark Weiser, 1991[1]

Abstract

There is a great deal of buzz surrounding the Internet of Things (IoT), which is the notion, simply put, that nearly everything not currently connected to the Internet from gym shorts to factories soon will be. The Industrial Internet of Things (IIoT) is one application of this trend and involves the use of IoT technologies in manufacturing. It holds the promise to revolutionize manufacturing, but there are a number of outstanding cybersecurity and data privacy issues impacting the realization of the myriad benefits promised by IIoT proponents. This white paper analyzes some of these, focusing on: (1) critical infrastructure protection and cybersecurity due diligence, (2) trends in transatlantic data privacy protections, and (3) the regulation of new technologies like artificial intelligence (AI) and blockchain. The paper concludes with a list of options for state and federal policymakers to consider in an effort to harden the IIoT along with the supply chains critical to the continued development of smart factories.

Introduction

In 2015, for only the second time in history to that point, a cyber attack was confirmed to have caused physical damage.[2] This time, the target was not Iran's nuclear program, but a steel mill in Germany. Specifically, a blast furnace was compromised causing "'massive' – though unspecified – damage."[3] Attackers had gained access to the plant through the firm's business network, highlighting the insecurity that can stem from interconnected systems even when a firewall is in place. There have been unconfirmed reports of similar incidents, such as one involving a petrochemical factory that was compromised by a coffee maker.[4] This issue is coming to the fore with

* *Scott J. Shakelford is Chair, Indiana University-Bloomington Cybersecurity Program; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; and Associate Professor, Indiana University Kelley School of Business.*

the expansion of Internet-connected devices in the manufacturing sector, which promise new efficiencies and innovations while also introducing new vulnerabilities.[5]

There is a great deal of buzz surrounding the Internet of Things (IoT), which is the notion, simply put, that nearly everything not currently connected to the Internet from gym shorts to factories soon will be.[6] McKinsey Consulting, for example, has estimated the economic impact of the Internet of Things, or what may be more accurately described as the "Network of Things,"[7] at $6.2 trillion by 2025.[8] The Industrial Internet of Things (IIoT), sometimes also called the "Factory of Things," or "Smart Factory Wave," is one facet of this trend toward an "embedded infosphere" and involves the use of IoT technologies in manufacturing applications.[9] It holds the promise to revolutionize manufacturing, including in the fields of "factory health, digital thread, and smart products."[10] Already, a number of industrial control systems (ICS) manufacturers such as Rockwell Automation are offering a range of IIoT products from programmable controllers and industrial sensors to distributed control systems.[11] However, while such products promote efficiency, they also increase the attack surface and with it the cyber risk that manufacturers must manage.[12]

There are a number of outstanding cybersecurity and data privacy issues impacting the realization of the myriad benefits promised by IIoT proponents, including the use of personal data in factory settings.[13] This paper analyzes some of these, focusing on: (1) critical infrastructure protection and cybersecurity due diligence, (2) trends in transatlantic data privacy protections, and (3) the regulation of new technologies like artificial intelligence (AI) and blockchain. The paper concludes with a list of options for state and federal policymakers to consider in an effort to harden the IIoT along with the supply chains critical to the continued development of smart factories.

Cybersecurity and Data Privacy IIoT Hot Topics

Although there are differing accounts as to the origin story of the term "Internet of Things," most accounts point to Kevin Ashton coining it in the form of a title for a 1999 presentation for Procter & Gamble.[14] But the idea has been around for longer, including as pervasive computing, "Ubiquitous Computing," and "Ambient Intelligence."[15] Although these terms are not all analogous,[16] it is true that from these humble beginnings has come a global effort to make our technology, businesses, and even our bodies, smart.[17] Wherever it came from, the term IoT today now enjoys widespread use in both technology and policy circles, as well as in popular culture.[18] But, in fact, it includes a constellation of devices and technologies with built-in wireless connectivity that "can be monitored, controlled[,] and linked"[19] together.

As more and more devices – not just computers and smartphones, but thermostats and lightbulbs – are connected to the Internet, the growing scale of the threat from hackers can easily get lost in the excitement of lower costs and smarter tech.[21] This section explores some of these security implications in the smart factory revolution, what has been called the "fourth revolution" in this space, before moving on to analyzing the associated policy implications.[22]

Smart Factories and Critical Infrastructure Protection

The United States has long grappled with the appropriate mix of laws and policies to help safeguard vital industries, which the Department of Homeland Security is tasked with defining and defending in the U.S. context to include 16 sectors.[23] These sectors are not fixed; for example, elections were included under the public facilities sector in January 2017.[24] Smart factories fall under an array of critical infrastructure sectors, including the critical manufacturing sector itself (which comprises electrical equipment and appliances along with transportation) along with the communications, healthcare, and even the defense industrial base. As such, firms operating in this space should be aware of the possibility for substantial federal oversight, such as would have been required under the Cybersecurity Act of 2012.[25] Each of these 16 sectors boasts an Information Sharing and Analysis Center (ISAC) to help spread cyber threat information, along with awareness as to best practices. Efforts

have also been made to break down silos between sectors, such as through Information Sharing and Analysis Organizations (ISAOs). Such public-private bi-directional information sharing between the critical infrastructure sectors will be critical to defending the IIoT, including both information technology (IT) (e.g., business systems) and operations technology (OT) that cover those systems in the manufacturing environment.[26] The latter distinction is important since IT efforts typically prioritize their focus on confidentiality, integrity and then availability, while OT efforts place the highest priority on availability. Compounding the challenge is that most existing OT systems do not have the capacity to add cybersecurity protections without negatively impacting production. This will be all the more important as threats to smart factories proliferate.

Threats from Foreign Nation-States and Economic Espionage Campaigns. In March 2018, the FBI and DHS jointly accused the Russian government of a "multi-stage intrusion campaign" targeting the U.S. power grid along with compromising the industrial control systems of several "small commercial facilities."[27] This episode is merely the latest in a string of cybersecurity incidents that involve U.S. critical infrastructure (CI) and that have been linked to Russia. Already, a number of nations have seen their systems compromised by such attempts, such as Ukraine, which experienced several of its substations crashing in December 2015 in "the first-ever confirmed cyberattack against grid infrastructure."[28] Unfortunately, the same pattern played out in Ukraine on December 23, 2016.[29] And Russia is not alone, with the list of cyber powers growing to more than 50 nations, not to mention sophisticated criminal organizations, firms, and hacktivists. Iran, for example, has reportedly readied a wave of cyber attacks against U.S. critical infrastructure in response to the U.S. withdrawal from the Iran nuclear agreement.[30] And the threat of cyber conflict is also only one facet of the multi-faceted cyber risk facing smart factories with the continued prevalence of trade secrets theft even after the U.S.-China 2015 Cybersecurity Code of Conduct, which was designed to safeguard commercial intellectual property and was prompted in part by hackers targeting U.S. Steel.[31] The rise of IIoT generally, and smart factories in particular, only expands the threat surface against which manufacturers will have to protect their systems and property necessitating advances in cybersecurity due diligence. In one demonstration, for example, a single compromised wireless webcam was able to "jam all wireless communication and thereby stop production" at a factory.[32] Other threats are numerous and can emanate from an array of actors including criminal organizations and terrorist groups, including insider threats and intellectual property theft.[33]

Meaning of "Cybersecurity Due Diligence" for Smart Factories. In the private-sector transactional context, cybersecurity due diligence has been defined as "the review of the governance, processes and controls that are used to secure information assets."[34] This increasingly central concept to a variety of business activities as it is used here builds from this definition and may be understood as the corporate, national, and international obligations of both State and non-State actors to help identify and instill cybersecurity best practices and effective governance mechanisms so as to promote cyber peace.[35] Put more simply, due diligence refers to an organization's activities to identify and understand the various risks it faces. Cybersecurity due diligence, then, is centered on risk management best practices and obligations that may exist between States, between non-State actors (e.g., private corporations, end-users), and between State and non-State actors, and refers to the international obligations of both State and non-State actors to help identify and instill cybersecurity best practices so as to promote security in the Factory of Things. The question becomes how can manufacturers fulfill these responsibilities, which include not just protecting technical infrastructure, but also safeguarding sensitive personal data that may be subject to big data analytics and deep learning, which is the topic we turn to next.[36]

Federal Cybersecurity Frameworks and Standards Impacting Smart Factories. Two of the main efforts aimed at defining cybersecurity due diligence that are most relevant to the smart factory context are the NIST Cybersecurity Framework (CSF), and the Federal Trade Commission's (FTC) guidance. First, the NIST CSF was born of frustration with the lack of action from Congress on cybersecurity, leading President Obama to empower NIST to partner with industry and develop a framework comprised of private-sector cybersecurity best practices that would help guide firms of all sizes, but particularly critical infrastructure operators.[37] The result was the first 2014 NIST CSF, which is critical since—even though it has been criticized as leading to a reactive

stance[38]—it is spurring the development of a baseline standard of cybersecurity due diligence in the United States.[39] In particular, the NIST CSF harmonizes industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk. Instead of the NIST CSF replacing organizations' existing security policies, NIST has intended for the Framework to provide support by helping organizations "identify, implement, and improve cybersecurity practices, and create a common language for internal and external communication of cybersecurity issues."[40] Although the NIST CSF was only published in 2014,[41] already some private-sector clients are receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST CSF."[42] Over time, the NIST CSF not only has the potential to shape a standard of care for domestic critical infrastructure organizations but also could help to harmonize global cybersecurity best practices for the private sector writ large given active NIST collaborations with more than twenty nations including the United Kingdom, Japan, Korea, Estonia, Israel, and Germany.[43] This progress has continued with the publication of Version 1.1 of the NIST CSF in April 2018, which, as Secretary of Commerce Wilbur Ross has argued "should be every company's first line of defense."[44] The new version boasts significant improvements, including with regards to authentication, supply chain cybersecurity, and vulnerability disclosure, though it is still best considered a cybersecurity floor rather than a ceiling.[45] It does not, for example, focus on IoT issues in particular, which is an area that many would like NIST to address in more detail as is discussed below.

Similar to NIST, the FTC recommends "tackling cybersecurity and all consumer-facing software development efforts with a holistic approach that incorporates a 'privacy by design' strategy to address the entire life cycle of data collection, use, access, storage, and ultimately secure data deletion."[46] The FTC has authority, granted in Section 5 of the Federal Trade Commission Act establishing the FTC, to create rules to block "unfair or deceptive acts or practices" on the part of companies doing business in the United States.[47] It has interpreted this authority in a way that permits it to level penalties against companies whose cybersecurity is not up to par if the company implies or advertises that they use certain cybersecurity practices, or if they operate in at-risk critical infrastructure sectors such as healthcare. This FTC interpretation was upheld by the U.S. Court of Appeals for the Third Circuit in 2015 in *FTC v. Wyndham Worldwide*.[48] However, based on a recent case, *LabMD Inc. v. Federal Trade Commission*, the FTC may need to become more specific in the cybersecurity standards it requires of businesses. This could include requiring more firms to take measures that so far the FTC has only encouraged on a voluntary basis, including:

1. Build security into devices at the outset, rather than as an afterthought in the design process;
2. Train employees about the importance of security, and ensure that security is managed at an appropriate level in the organization;
3. Ensure that when outside service providers are hired, that those providers are capable of maintaining reasonable security, and provide reasonable oversight of the providers;
4. When a security risk is identified, consider a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk;
5. Consider measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on the network;
6. Monitor connected devices throughout their expected life cycle, and where feasible, provide security patches to cover known risks.[49]

However, due to complex supply chains and a global customer base, U.S. federal IoT regulations are by no means the only ones that IIoT proponents must consider. The next section considers the impact of the State of California's recent efforts before moving on to discuss the European Union's regulatory efforts at cybersecurity and data privacy on the smart manufacturing sector.

State-Level IIoT Policy: California Case Study. As with its groundbreaking 2002 privacy law that ushered in the first data breach notification standards, an idea that has since been copied by the other 49 states and the European Union as is discussed further in the next subsection, California's 2018 Consumer Privacy Act is helping to set a new standard for U.S. privacy protections. Although it does not go quite as far as the EU's new General Data Protection Regulation (GDPR) discussed below, it does include provisions that allow consumers to sue over data breaches, and decide when, and how, their data is being gathered and used by companies.[50] Although there remains debate about the scope and effectiveness of this intervention,[51] the law may well help shape the cybersecurity practices of the manufacturing base in California along with their business partners, such as by requiring added efforts to protect the privacy rights of consumers and suppliers.

This law builds on California's existing IoT policies. For example, in January 2016, California expanded its definition of the term "personal information" to include "a person's name in combination with his or her Social Security number, driver's license or [state] identification card, credit or debit card number and password, or medical information."[52] In fact, some commentators suggest that "[w]hen the amendments take effect, 'personal information' will also include a person's name coupled with his or her health insurance information, and a username or email address in combination with a password or security question and answer that would permit access to an online account."[53] In addition, California law will now require "companies that share such information to not only take extra security precautions themselves when managing the information, but also to ensure that any entities they share information with also abide by strict security measures."[54] The implications of this "sharing information forward" regulation are expansive in that it creates two broad categories of businesses "those which own, license, or maintain personal information about California residents, and businesses which, pursuant to contract, disclose personal information about California residents to unaffiliated third parties."[55] In practical effect, the regulation will require businesses to include within third part information sharing agreements "contractual provisions mandating implementation of reasonable security measures."[56] This could, for example, have the effect of further spreading both the NIST CSF and the FTC cybersecurity efforts discussed above. An accounting of state-level cybersecurity laws as of July 2018 is included in Appendix A.

Transatlantic Approaches to Data Privacy in the Industrial IoT Context

The European Union has long taken a distinct and far more regulatory and comprehensive approach to both cybersecurity and data privacy protection as compared to the sector-specific regime preferred in the United States.[57] This fact may be seen in 2018 with the passage of the Network Information Security (NIS) Directive, and the enactment of GDPR, both of which are explored in this section. The EU approach is not without its critics, such as those who are concerned about over-centralization,[58] but it is equally true that these efforts have made the EU a global leader in information governance best practices.[59] Moreover, it should also be noted that transatlantic approaches to how organizations should manage their cyber risk are converging around the language of risk management, as may be seen by the EU's Network Information Security Public-Private Platform (NIS Platform), which specifically adopts the NIST CSF core—identify, protect, detect, respond, recover—as the industry-standard EU approach for cybersecurity risk management.[60] The 2013 EU Cybersecurity Strategy introduced the Network Information Security (NIS) Directive's goal to "facilitate exchange of best practices," enhance "risk management practices and information sharing"[61] through the establishment of the NIS Platform.[62] This Platform helped collect "existing risk management standards and best practices" [63] that organizations "can use and tailor to their own approach to risk management."[64]

As with cybersecurity and information privacy generally, the EU has long been engaged with IoT issues in particular dating back at least to 2009.[65] As one example, in 2014 the European Commission funded a project named CIPHER, which had the goal of conducting an "in-depth analysis of the reality of security in privately held information systems in Europe."[66] Specifically, CIPHER included an effort to draft a regulatory roadmap with recommendations for policymakers that included IoT.[67] The European Commission has also founded the Alliance for Internet of Things Innovation, which has been tasked with developing a large-scale framework specifically

addressing issues within IoT.[68] The group has also engaged internationally, welcoming delegations from around the world to discuss IoT governance,[69] reinforcing the EU's place as a key hub for cybersecurity and privacy governance. Finally, in late 2015 the European Commission launched Horizon 2020, which included goals for smart cities and IoT deployment.[70] In short, the EU is embracing the 'Internet of Everything,' including wearables, which are "integrating key technologies (e.g. nano-electronics, organic electronics, sensing, actuating, localization, communication, energy harvesting, low power computing, visualization and embedded software) into intelligent systems to bring new functionalities into an array of consumer products including clothes, fabrics, patches, watches and other body-mounted devices."[71] These goals demonstrate how the EU is planning to secure the full gambit of IoT devices, including those in the manufacturing sector.[72]

Impact of GDPR. A key aspect for how the EU will shape IoT governance is through the General Data Protection Regulation (GDPR), which is an extension of its long push to create a Digital Single Market (DSM). Although most of the press coverage of the GDPR has focused on its privacy protection regulations and the potentially very large penalties that can be imposed for not following the data privacy rules, an important goal of the GDPR is to tear down, to the extent feasible, remaining regulatory walls between the EU Member States and move toward a single EU market.[73] Similar to the NIST CSF, which "relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience,"[74] the DSM synthesizes initiatives on security and data protection.[75] Most importantly, the DSM focuses its approach upon considerations of the "data economy (free flow of data, allocation of liability, ownership, interoperability, usability and access), and thus promises to tackle interoperability and standardization" that are issues critical to boosting the securing in the Factory of Things.[76]

Building from this foundation, GDPR is an expansive regulatory regime with a wide array of requirements on covered firms ranging from ensuring data portability and consent to mandating that firms disclose a data breach within 72 hours of it becoming aware of the incident and then conducting a post mortem to ensure that a similar scenario will not recur.[77] As groundbreaking as these regulations are, though, they were not drafted with IoT in mind, despite a 2017 finding by the European Union Agency for Network and Information Security (ENISA) "that there were no 'legal guidelines for IoT device and service trust.' Nor any 'level zero defined for the security and privacy of connected and smart devices.'"[78] Further, European-level regulation is slow, and a blunt instrument –GDPR, as one example, took more than four years to be adopted after having been proposed in 2012.[79]

For manufacturing firms, as has been argued by Microsoft, "[t]he message is clear: manufacturers, even outside Europe, need to consider their exposure under the GDPR and plan accordingly."[80] More specifically, according to Olivier Van Hoof of Collibra:

> [GDPR] has particular relevance for the manufacturing industry, which is using AI and RFID [Radio Frequency Identification] to collect, use and integrate personal information into product manufacturing. Through IoT and their quest to make better connections with end users, manufacturers are collecting more information about consumers. And we've seen a number of studies indicating the manufacturing industry lags behind in cybersecurity. Therefore, specific safeguards should be established for these newer forms of electronic communications and sharing of personal data. And it shouldn't be taken lightly. Regulators will issue significant fines for GDPR non-compliance, up to 2-4% of global revenue for non-compliance. The deadline for compliance . . . [was] May 25, 2018.[81]

Applicability of NIS Directive to Smart Factories. Directives such as the NIS Directive have the benefit of providing more freedom to nations to craft solutions to common problems, such as the need for more robust critical infrastructure protection, but this can similarly be a cumbersome process.[82] The process that led to the NIS Directive is similar to deliberations involving the NIST CSF, which included "four public-private partnerships in which hundreds of businesses and policymakers from the U.S. and around the world got together to build and revise the NIST Framework, showing a remarkable ability to build consensus across numerous sectors and stakeholders in a complex and dynamic arena."[83] Many commentators argue that this "type of active industry

dialogue is a crucial piece of the NIST Framework's success—as well as that of the more general bottom-up approach to cybersecurity regulation—in the United States, and is one that other nations are seeking to emulate."[84] For example, the French government is considering mandating liability for security lapses on the part of IoT manufacturers.[85]

Applicability of Blockchain Technology to Managing Supply Chain Risks

It is common knowledge that hackers can attack software by sending users virus-infected emails or compromised links.[86] But they can also meddle with computers by altering tiny circuits in microchips most users will never see.[87] These weaknesses are physical, but they are just as hard to identify as mistakes in software code. In fact, the complex supply chains involved in most technological manufacturing are very hard to secure. Apple's iPhone, for example, involves hundreds of suppliers from around the world making chips and hard drives, all of which have to be shipped, assembled, and warehoused before ever being delivered to an Apple store, or your front door.[88] All of these steps introduce opportunities for security problems to arise; recent research has even suggested that hackers could use smartphone apps to damage manufacturing equipment, or even destroy entire factories.[89] While no such large-scale disaster has yet taken place, even sophisticated retailers like Amazon have been fooled by counterfeit or poorly manufactured facsimiles of real products.[90] Some supply chain threats can be more malicious; in 2012, Microsoft warned customers that Chinese computer factories were installing malware on PCs before they even left the production line.[91] Even innocent motives may underlie serious problems. In 2015, Lenovo installed advertising software on its computers, dangerously weakening system security.[92] These issues are particularly problematic in the IIoT context as more tech is deployed in factories, expanding economic opportunities as well as the attack surface.

As more and more industrial devices are connected to the Internet, the growing scale of the threat from hackers could easily be eclipsed by excitement over lower costs and smarter tech.[93] One new way to secure supply chains involves blockchain tech—a secure database system stored and maintained across many computers around the internet—to track and verify all aspects of a complicated supply chain like Apple's. IBM and the international shipping giant Maersk are experimenting with using blockchain systems to better secure and transparently track shipments, as well as automate payments.[94] This is one of the benefits of blockchain tech since the distributed smart contracts that these systems generate are automatically enforceable. Once a component part like a chip is delivered, for example, a blockchain verifies that fact and the supplier automatically is paid in dollars, or their cryptocurrency of choice. But no blockchain is immune to hacking—and none can evade the effects of hardware vulnerabilities like Meltdown and Spectre.[95] Further, policymakers around the world are taking a hard look at appropriate blockchain regulations, with divergent approaches being tried from Albany to Brussels.[96]

Role for Policymakers

Policymakers at the state and federal level can help manufacturing firms better manage the multifaceted cyber threat facing smart factories. This Part discusses some available options, beginning with civil society and insurance before moving on to standards bodies and finally an analysis of pending bills before Congress and the importance of fostering international dialogue.

Instilling Cybersecurity Risk Management Best Practices

Instead of black letter regulation, many, particularly in industry, prefer self-regulation with the flexibility "to adapt to rapid technological progress"[97] Such self-regulation has the capacity to adapt better and faster than black letter law to rapidly changing technological and social forces. It can also be efficient and cost-effective than command and control-style regulation,[98] though it is not a panacea.[99] Still, one organization that is trying to create such a community is *Consumer Reports*. Specifically, in March 2017 *Consumer Reports* launched its

Digital Standard, which is designed "to measure the privacy and security of products, apps, and services will put consumers in the driver's seat as the digital marketplace evolves."[100] Once it fully matures, the Digital Standard could help empower consumers to select products—including in the IoT context—that meet rigorous privacy and security requirements. But, since *Consumer Reports* is not a regulatory organization, vendors will still be legally able to sell products that do not meet the Standard. Over time, a best-case scenario is that the Standard holds the promise of helping the market function more efficiently by rewarding those firms that take cybersecurity and data privacy seriously, and penalizing those that do not through lower scores and, as a result, less revenue. Already, these efforts are having an impact, such as when it helped expose privacy risks in the pregnancy and fertility app Glow.[101] As the Digital Standard is continually refined, and globalized, it will likely further impact the trajectory and rate of global IoT privacy and security standards, including those available to manufacturers.[102]
The insurance industry is similarly helping to incentivize the uptake of cybersecurity best practices. Insurance has been called a "key part of the [cybersecurity] solution," but it has only recently begun to catch on, albeit in fits and starts.[103] After all, insurance is a primary way that we as a society manage risky behavior across myriad sectors, from car accidents to health care. Indeed, according to Roger Smith of Allianz, "Cyber insurance is probably the fastest growing insurance in the world."[104] By some estimates the market will be worth more than $7.5 billion by 2020 with an increasing number of firms looking to invest in coverage,[105] a trend that could be reinforced depending on regulatory developments such as the Securities and Exchange Commission (SEC) cyber attack disclosure guidelines.[106] Yet calculating cyber risk insurance premiums is no simple matter—there is little reliable data that is so critical,[107] for example, to pricing healthcare and automobile insurance. Some discounts are available, though, to help with spiraling costs; Bryce and AIG, for example, have a history of offering rebates for firms using secure hardware and software packages. Other insurers are going further. Ben Beeson of Lockton Companies, for example, has stated that, "Insurers are promoting newer technologies for securing payment card transactions that exceed credit card companies' requirements, such as tokenization and end-to-end encryption."[108] Over time, such efforts could help ratchet up the overall level of cybersecurity preparedness across a range of businesses, including manufacturing, though it is important to understand that such coverage is only part of the solution, and that it is vital to review coverage terms lest patchy policies contribute to an inaccurate and reactive mindset on the part of covered firms.[109]

Role of Cybersecurity Standards Bodies

Beyond the general NIST CSF, NIST has also released another Framework focusing on IoT issues entitled the "Framework for Cyber-Physical Systems" ("NIST IoT Framework") in September 2015.[110] In essence, the NIST IoT Framework "is intended to serve as a common blueprint for the development of safe, secure, and interoperable systems as varied as smart energy grids, wearable devices, and connected cars."[111] Moreover, the Framework is also meant "to help manufacturers create new [Cyber-Physical Systems] that can work seamlessly with other such smart systems that bridge the physical and computational worlds."[112] Similar to the 2014 NIST CSF, the 2015 NIST IoT Framework was developed through a multi-stakeholder process and proposes to enhance the security of things by "providing a common set of considerations for the design of devices and a common language to allow designers to promote interactions between devices."[113] As with the NIST CSF, the NIST IoT Framework is a risk-based approach to managing cyber risk targeted at the IoT context. The goals of the NIST IoT Framework are to "derive a unifying framework that covers . . . the range of unique dimensions of CPS."[114] To aid in these goals, the NIST IoT Framework identifies cyber-physical systems (CPS) domains as well as analyzing and addressing cross-cutting concerns.[115] Although both the 2014 NIST CSF and the 2015 NIST IoT Framework could help regulate IoT through the courts such as by helping to define a standard for cybersecurity care in IoT negligence actions,[116] some argue that the existing NIST IoT Framework is not specific (or user-friendly) enough to make the same impact on IoT as the NIST CSF has had on critical infrastructure protection.

Federal Policy Options

An array of policy options are being discussed at the federal level that would impact the growth and development of IIoT applications. This section focuses on the most recent proposed IoT bill, a repackaged Privacy Bill of Rights, as well as the active defense debate.

Proposed IoT Bill. Senators Mark Warner, Cory Gardner, Ron Wyden, and Steve Daines introduced the Internet of Things Cybersecurity Act of 2017 with this aim in mind. In brief, the legislation would require vendors who sell products to the U.S. government to: (1) ensure that their devices "are patchable," (2) that they do not "contain known vulnerabilities," that they "rely on standard protocols," and (4) they "don't contain hard-coded passwords."[117] However, the bill does not take a one-sized-fits-all to regulating an area as vast as IoT. Indeed, the authors provide a path forward whereby, if industry provides "equivalent, or more rigorous, device security requirements" then they may be utilized in lieu of the foregoing.[118] The legislative effort has a long list of proponents from Bruce Schneier and Professor Jonathan Zittrain to leading voices from Symantec and the Center for Democracy and Technology,[119] but also has its share of critics.[120] Overall, though, the bill only has a 13 percent chance of becoming law as of June 2018, according to Skopos Labs,[121] leading one to consider alternatives.

Privacy Bill of Rights. As with California's 2018 Consumer Privacy Act, there are similar proposals at the federal level to codify some of the protections from GDPR discussed above for U.S. consumers. This Privacy Bill of Rights, a version of which was first trumpeted by the Obama Administration in 2012, was part of the CONSENT (Consumer Online Notification for Stopping Edge-provider Network Transgressions) Act introduced by Senate Democrats in 2018 in the wake of the Cambridge Analytica scandal.[122] If enacted, the law would require covered firms "to obtain opt-in consent from users before sharing, selling or otherwise using their personal information . . . [along with] develop[ing] reasonable data security practices."[123] It would impact manufacturers directly since its cybersecurity and data processing requirements would apply not just to social networks, but to an array of publicly traded firms including those deploying IIoT tech.

Graves Bill. As of June 2018, Congress was considering a wide range of cybersecurity legislation from a privacy bill of rights,[124] to election security,[125] but included in this list is the Active Cyber Defense Certainty (ACDC) Act, also known as the Graves Bill after Congressman Tom Graves, a Republican from Georgia, whom introduced it. As of June 2018, the bill had nine co-sponsors from both political parties, and even though its imminent passage is unlikely at least in its current form, it has received sufficient attention to analyze in some detail.[126] Specifically, the ACDC Act would permit firms to operate beyond their network perimeter, including the potential to conduct surveillance on entities "who are thought to have done hacking in the past or who, according to a tip or some other intelligence, are planning an attack."[127] The bill also clarifies "the type of tools and techniques that defenders can use that exceed the boundaries of their own computer network."[128] In particular, it specifies that people facing criminal charges under the CFAA for illegal hacking can defend themselves by claiming that their activities were "active cyber defense measures."[129] According to the bill's text, the accused would have to show that they were the victims of a "persistent unauthorized intrusion" directed at their computers.[130] In summary, according to Congressman Graves, "This is an effort to give the private sector the tools they need to defend themselves[.]"[131] If enacted, such a policy would allow manufacturers to potentially target foreign sponsors of cyber attacks.

Concerns regarding the ACDC Act, though, fall across several dimensions, summarized in Table 1. Some, such as former NSA Directors Admiral Michael S. Rogers and Keith Alexander, are concerned about further complicating an already complex cyber threat landscape.[132] Others, such as Joyce, are more concerned about sanctioning "vigilantism" which could, he argued, even in a best-case scenario lead to unqualified actors bringing risk to themselves, their targets, and their governments."[133]

Table 1. Advantages and Disadvantages of Active Defense[134]

Advantages	Disadvantages
More advanced knowledge of potential threats and the attacker's capabilities and intent, which helps to mitigate surprise and protect assets	Backfiring due to human error or manipulation by the attacker
Greater range of options to engage the attacker, including flexibility in where, when, and how	Collateral damage as a result of disrupting or damaging an innocent third-party computer or network or wrongly attributing the source of an attack
Enhanced ability to disrupt or shut down a planned or ongoing operation even after the initial penetration of the defender's network	Escalation in an exchange between attacker and defender as a result of the attacker's response to ACD measures
Increased likelihood of deterring future attacks by complicating the attack, impeding the use of data, and raising the direct and indirect costs to and risk for the attacker (especially in being identified)	Uncertain strategic implications, including the potential political and legal consequences of measures affecting external networks

Opportunities for International Norms Development

There are many ways to conceptualize cybersecurity policy in the Factory of Things, but among them is the dynamic field of polycentric governance. This governance framework may be considered to be a multi-level, multi-purpose, multi-functional, and multi-sectoral model[135] that has been championed by numerous scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, which challenges orthodoxy in part by demonstrating the benefits of self-organization and networking regulations "*at multiple scales*."[136] It also posits that, due to the existence of free riders in a multipolar world, "*a single governmental unit*" is often incapable of managing "global collective action problems"[137] such as cyber-attacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[138] Such an approach, in other words, recognizes both the common but differentiated responsibilities of public- and private-sector stakeholders as well as the potential for best practices to be identified and spread organically generating positive network effects that could, in time, result in the emergence of a norm cascade improving smart factory security.[139]

One example of a successful public-private polycentric collaboration is the NIST CSF, which, as has been noted, is now going global. The success of such frameworks, civil society efforts like the *Consumer Reports Digital Standard*, and regional regimes like GDPR, is part and parcel of the literature on polycentric governance. However, it is important to note that not all polycentric systems are guaranteed to be successful. Disadvantages, for example, can include gridlock and a lack of defined hierarchy.[140] The Ostrom Design Principles can help predict the institutional success of given interventions.[141] Still, the literature remains immature, as does the current state of IoT governance. In fact, the Information Systems Audit and Control Association (ISACA)[142] surveyed IT professionals in the United Kingdom and found that "75 percent of the security experts polled say they do not believe device manufacturers are implementing sufficient security measures in IoT devices, and a further 73 percent say existing security standards in the industry do not sufficiently address IoT *specific* security concerns."[143]

Manufacturing firms should engage in these conversations, for example to build on the progress of making attacks on civilian critical infrastructure—including smart factories—off limits, as well as by investing in both security and privacy by design. This involves further refining the scope of cybersecurity due diligence at the international level, as well as boosting public-private information sharing, and even recasting the cybersecurity debate in the manufacturing sector as not just an exercise in cost-benefit analysis, but as a corporate social

responsibility. Already, Eli Lilly has come out in support of this shift by incorporating cybersecurity and data privacy findings into its integrated sustainability report, along with complying with GDPR requirements globally. Other firms could learn from this example and build on the progress that has already been made regarding the Cybersecurity Tech Accord.[144]

Conclusion

As the IIoT matures, disparate commercial networks will be able to communicate with one another, creating smart (and potentially more resilient) things, factories, and societies. Such an ultimate, macro-level outcome resembles the early days of networking when Cisco used multi-protocol routing to join dissimilar networks that eventually led to the widespread adoption of a common networking standard called the Internet Protocol, which we all rely on today every time we sign online. IoT looks set to follow a similar route, albeit on a larger scale, spanning myriad sectors and industries. In response, polycentric IoT cybersecurity regulations should be adapted and improved to better keep pace with these changes,[145] particularly with regards to data regulations monitoring private firms and public-sector organizations that transfer PII.[146] This includes frameworks and standards—including a NIST IoT-specific effort—along with the Cons*umer Reports* Digital Standard, and the use of corporate governance structures, such as sustainability, and international norms, including due diligence. Such an all-of-the-above polycentric approach is essential to addressing governance gaps in smart factories as part of improving security and data privacy in the ever-expanding Internet of Everything.

Works Cited (Endnotes)

1 Mark Weiser, 1991. "The Computer for the 21st Century," *Sci. Am.* https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf.

2 The first such episode was Stuxnet. See Kim Zetter, 2014. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired* (Nov. 3), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

3 Kim Zetter, 2015. "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired* (Jan. 8), https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

4 See "How the Coffee-Machine Took Down a Factories Control Room," 2017, *Reddit*, https://www.reddit.com/r/talesfromtechsupport/comments/6ovy0h/how_the_coffeemachine_took_down_a_factories/.

5 These include Distributed Denial of Service (DDoS) attacks and botnets such as Mirai. See Constantinos Kolias et al., 2017. "DDoS in the IoT: Mirai and Other Botnets," 50 *IEEE Computer* 80, 80.

6 For more on this topic, see Scott J. Shackelford et al., 2019 (forthcoming). "When Toasters Attack: Enhancing the 'Security of Things' through Polycentric Governance," 2017 *Univ. Ill L. Rev.* 415; Scott J. Shackelford & Scott Bradner, "Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything," __ *Eur. J. Int'l L.* __.

7 Jeffrey Voas, 2016. "Demystifying the Internet of Things," 49 *IEEE Computer* 40, 42, http://wmcyberintrusion.info/wp-content/uploads/2017/11/DemystifyingIoT2016.pdf.

8 Chunka Mui, "Thinking Big About The Industrial Internet Of Things," 2016. *Forbes* (Mar. 4), https://www.forbes.com/sites/chunkamui/2016/03/04/thinking-big-about-industrial-iot/#7f1e54066220.

9 Richard D. Taylor, 2017. "The Next Stage of U.S. Communications Policy: The Emerging Embedded Infosphere," 41 T*elecom Pol'y* 1039, 1040 (arguing that "[t]he United States needs to reimagine the basic principles of its telecommunications and information policy to fit an emerging society in which networking and intelligence are embedded into an increasing number of everyday things which constantly monitor and measure our lives. This emerging environment is an always-on, ubiquitous, integrated system comprised of the Internet of Things, Big Data, Artificial Intelligence/Intelligent Systems and the Intercloud, which act together as a single system, referred to here as the 'Embedded Infosphere' (EI).").

10 Mui, *supra* note viii.

11 See Product Offerings, Rockwell Automation, https://www.rockwellautomation.com/en_NA/products/overview.page (last visited Sept. 23, 2018).

12 See Bob Tarzey, 2017. "The Ever-Growing IoT Attack Surface," *Computer Wkly* (July 6), https://www.computerweekly.com/blog/Quocirca-Insights/The-ever-growing-IoT-attack-surface.

[13] One application of this concept is the personalized medicine movement and the fact that high-risk personal data are typically not covered under HIPAA. See, e.g., Randy Vogenberg et al., 2010. "Personalized Medicine," 35 *Pharmacy & Therapeutics* 624, 626, 628-631, 642.

[14] Kevin Ashton, 2009. "That 'Internet of Things' Thing," *RFID J.* (June), www.rfidjournal.com/articles/view?4986.

[15] See Jackie Fenn and Hung LeHong, 2011. "Hype Cycle for Emerging Technologies," *Gartner* (July 28), https://www.gartner.com/doc/1754719/hype-cycle-emerging-technologies-; Detlef Zuehlke, "Smart-Factory: Towards a Factory-of-Things," 2010. 34 *Ann. Rev. Control* 129-38, http://www.sciencedirect.com.proxyiub.uits.iu.edu/science/article/pii/S1367578810000143 [https://perma.cc/QN6X-LEAA].

[16] See Jennifer Sunrise Winters, 2018. "Privacy, Algorithmic Discrimination, and the Internet of Things," in *Encyclopedia of Information Science and Technology* 4951, 4952 (Medhi Khosrow-Pour ed.).

[17] See, e.g., Meghan Neal, 2014. "*The Internet of Bodies is Coming, and You Could Get Hacked*," *Motherboard* (Mar. 13), https://motherboard.vice.com/en_us/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked.

[18] Fenn and LeHong, *supra* note xv.

[19] Bonnie Cha, 2015. "A Beginner's Guide to Understanding the Internet of Things," *Recode* (Jan. 15, 2015), https://www.recode.net/2015/1/15/11557782/a-beginners-guide-to-understanding-the-internet-of-things.

[20] Technologies, 2016. "Underpin the Hype Cycle for the Internet of Things, 2016," *Gartner* (Nov. 2), https://www.gartner.com/smarterwithgartner/7-technologies-underpin-the-hype-cycle-for-the-internet-of-things-2016/.

[21] See Aaron Tilley, 2015. "How Hackers Could Use A Nest Thermostat As An Entry Point Into Your Home," *Forbes* (Mar. 6), https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#235d0d693986; Carl Franzen, 2017. "How to Find a Hack-Proof Baby Monitor," *Offspring* (Aug. 4), https://offspring.lifehacker.com/how-to-find-a-hack-proof-baby-monitor-1797534985; Charlie Osborne, 2015. "Smartwatch Security Fails to Impress: Top Devices Vulnerable to Cyberattack," *ZDNet* (July 22), http://www.zdnet.com/article/smartwatch-security-fails-to-impress-top-devices-vulnerable-to-cyberattack/; John Markoff, 2016. "Why Light Bulbs May B the Next Hacker Target," *N.Y. Times* (Nov. 3), https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r=0.

[22] For more information about smart factories and machinery, see Hyoung Seok Kang et al., 2016. "Smart Manufacturing: Past Research, Present Findings, and Future Directions," 3 *Int'l J. Precision Eng'g & Mfg.-Green Tech.* 111-28, http://link.springer.com.proxyiub.uits.iu.edu/article/10.1007/s40684-016-0015-5 [https://perma.cc/CA9L-738H].

[23] Presidential Policy Directive 21 (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. *What is Critical Infrastructure*, DHS, http://www.dhs.gov/what-critical-infrastructure (last visited Jan. 16, 2014); *What is the ICS-CERT Mission?*, http://ics-cert.us-cert.gov/Frequently-Asked-Questions (last visited Jan. 17, 2014) (The U.S. Cyber Emergency Response Team, which is part of DHS, identifies 16 critical infrastructure sectors consistent with Homeland Security Presidential Directive 7, including: agriculture, banking and finance, chemical, commercial facilities, dams, defense industrial base, drinking water and water treatment systems, emergency systems, energy, government facilities, information technology, nuclear systems, public health and healthcare, telecommunications, and transportation systems).

[24] "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," 2017. *Dep't Homeland Sec.* (Jan. 6), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[25] See Scott J. Shackelford, 2012. "In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012," 64 *Stanford Law Review Online* 106 (Mar. 8), http://www.stanfordlawreview.org/online/cyber-peace.

[26] See Amanda Ziadeh, 2018. "Homeland Security is Building Collective Defense Against Adversaries," *Govt. CIO Media* (July 20). https://www.governmentciomedia.com/homeland-security-building-collective-defense-against-adversaries.

[27] Taylor Hatmaker, 2018. "DHS and FBI Detail How Russia is Hacking into U.S. Nuclear Facilities and Other Critical Infrastructure," *Tech Crunch* (Mar. 15), https://techcrunch.com/2018/03/15/russia-energy-hack-dhs-fbi-us-cert/.

[28] Jeff St. John, 2017. "The Real Cybersecurity Issues Behind the Overhyped 'Russia Hacks the Grid' Story," *Greentech* (Jan. 4), https://www.greentechmedia.com/articles/read/the-real-cybersecurity-issues-behind-the-overhyped-russia-hacks-the-grid-st.

[29] See Thomas Fox-Brewster, 2016. "Ukraine Claims Hackers Caused Christmas Power Outage," *Forbes* (Jan. 4), http://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/#77b6ed5d5e6f.

[30] See Courtney Kube et al., 2018. "Iran has Laid Groundwork for Extensive Cyberattacks on U.S., Say Officials," *NBC News* (July 20), https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork-extensive-cyberattacks-u-s-say-officials-n893081.

[31] See Gary Brown and Christopher D. Yung, 2017. "Evaluating the US-China Cybersecurity Agreement, Part I: The US Approach to Cyberspace," *Tech. Diplomat* (Jan. 19), https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/; Colin Hanna, 2017. "China Stonewalls U. S. Steel's Cybertheft Lawsuit," *Investors* (Mar. 27), https://www.investors.com/politics/commentary/china-stonewalls-u-s-steels-cyber-theft-lawsuit/.

[32] For more on this topic, see Scott J. Shackelford, Scott Russell, and Andreas Kuehn, 2016. "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors," 17 *Chi. J. Int'l L.* 1.

[33] For more information on this topic, see Scott J. Shackelford et al., 2015. "Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets through Bilateral Investment Treaties," 52 *Am. Bus. L.J.* 1.

[34] Tim Ryan and Leonard Navarro, 2015. "Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks," *Kroll Call* (Jan. 28), http://blog.kroll.com/2015/cyber-due-diligence-pre-transaction-assessments-can-uncover-costly-risks/.

[35] For a discussion of cyber peace, see Scott J. Shackelford, *The Meaning of Cyber Peace,* Notre Dame Inst. Adv. Study Q. (2013), https://ndias.nd.edu/news-publications/ndias-quarterly/the-meaning-of-cyber-peace/.

[36] In general, data privacy policies are needed to cover proprietary manufacturing data generated by the IIoT. Such data may range from the code that runs machines to the output of sensors that measure recipe amounts and composition. There are a number of situations where such data may be captured and aggregated by supply chain partners, equipment manufacturers, and others. The lack of a clear delineation of ownership is an impediment for companies to connect their IIoT systems to each other, reducing the benefits of digital manufacturing.

[37] See *National Institute of Standards and Technology, Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework 1,* 2013. Available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

[38] Taylor Armerding, 2014. "NIST's Finalized Cybersecurity Framework Receives Mixed Reviews," *CSO* (Jan. 31), http://www.csoonline.com/article/2134338/security-leadership/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html.

[39] See, e.g., Scott J. Shackelford et al., 2015. *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 *Tex. J. Int'l L.* 287; Scott J. Shackelford, Scott Russell, and Andreas Kuehn, 2016. "Defining Cybersecurity Due Diligence Under International Law: Lessons from the Public and Private Sectors," 17 *Chi. J. Int'l L.* 1.

[40] *PwC, Why You Should Adopt the NIST Framework 1* (May 2014), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

[41] See "Framework for Improving Critical Infrastructure," 2015. *NIST* (Apr.), http://www.nist.gov/cyberframework/upload/cybersecurity_framework_bsi_2015-04-08.pdf (noting that "To allow for adoption, Framework version 2.0 is not planned for the near term.").

[42] "Why the NIST Cybersecurity Framework Isn't Really Voluntary," 2014. *Info. Sec. Blog* (Feb. 25), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

[43] There is some evidence that this may already be happening, including with regards to the Federal Trade Commission's cybersecurity enforcement powers. See, e.g., Brian Fung, 2015. "A Court Just Made it Easier for the Government to Sue Companies for Getting Hacked," *Wash. Post* (Aug. 24), https://www.washingtonpost.com/news/the-switch/wp/2015/08/24a-court-just-made-it-easier-for-thegovernment-to-sue-companies-for-getting-hacked/?wpmm=1&wpisrc=nl_headlines.

[44] "NIST Releases Version 1.1 of its Popular Cybersecurity Framework," 2018. *NIST* (Apr. 16), https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

[45] See *id*.

[46] See "FTC Enters 'Internet of Things' Arena With TRENDnet Proposed Settlement," 2013. *Info. L. Gp.* (Sept. 9), http://www.infolawgroup.com/2013/09/articles/ftc/trendnet-settlement/.

[47] FTC, "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority," 2008. *FTC*, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[48] W. Reece Hirsch et al., 2015. "Third Circuit Sides with FTC in Data Security with Wyndham," *Nat'l L. Rev.* (Sept. 8), https://www.natlawreview.com/article/third-circuit-sides-ftc-data-security-dispute-wyndham.

[49] "FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks," 2015. *Fed. Trade Comm'n* (Jan. 27), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices [hereinafter "FTC IoT Report"].

[50] See Ben Adler, 2018. "California Passes Strict Internet Privacy Law With Implications For The Country," *NPR* (June 29), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country?utm_source=facebook.com&utm_medium=social&utm_campaign=npr&utm_term=nprnews&utm_content=20180629.

[51] See Jeff Kosseff, 2018. "Ten Reasons Why California's New Data Protection Law is Unworkable, Burdensome, and Possibly Unconstitutional" (Guest Blog Post), *Tech. & Marketing L. Blog* (July 9), https://blog.ericgoldman.org/archives/2018/07/ten-reasons-why-californias-new-data-protection-law-is-unworkable-burdensome-and-possibly-unconstitutional-guest-blog-post.htm.

[52] Dan Cook, 2015. "New Privacy Regs in CA, NV Tighten Security Measures," *BenefitsPro*, (Aug. 12), http://www.benefitspro.com/2015/08/12/new-privacy-regs-in-ca-nv-tighten-security-measure.

[53] See *id*.

[54] *Id*.

[55] *Id*.

[56] *Id*.

[57] See, e.g., Scott J. Shackelford, 2018 (forthcoming). "Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations," ___ *Seton Hall J. of Diplomacy & Int'l Rel.* ___.

[58] Response to EU Cybersecurity Strategy and proposed Directive on Network and Information Security (NIS), EurActiv Press Release (Feb. 7, 2013), http://pr.euractiv.com/pr/response-eu-cybersecurity-strategy-and-proposed-directive-network-and-information-security-nis ("Member States are building communities and trust through local, regional, or sector specific private public partnerships, yet we see a general change in approach in the draft Network and Information Security Directive from working hand-in-hand with industry, to top-down, unidirectional reporting obligations and requirements.").

[59] No other nations, for example, have taken the U.S. approach to data privacy protection. See Mark Scott and Laurens Cerulus, 2018. "Europe's New Data Protection Rules Export Privacy Standards Worldwide, *Politico* (Jan. 31), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/.

[60] NIS Platform (WG-1) Final Draft 220515, Network and Information Security Risk Management Organizational Structures and Requirements, available at https://resilience.enisa.europa.eu/nis-platform/shared-documents/5th-plenary-meeting/chapter-1-nis-risk-management-organisational-structures-and-requirements-v2/at_download/file. For more on this topic, see Scott J. Shackelford, Scott Russell, and Jeffrey Haut, 2016. "Bottoms Up: A Comparison of 'Voluntary' Cybersecurity Frameworks," 16 Univ. Cal. Davis Bus. L.J. 217.

[61] *A Cyber Security Framework For Europe, Eur. Comm'n* (last updated on Aug. 5, 2014), http://cordis.europa.eu/news/rcn/121360_en.html.

[62] *ENISA, Network and Information Security Risk Management Organizational Structures and Requirements* 14 (2015), https://resilience.enisa.europa.eu/nis-platform/shareddocuments/5th-plenary-meeting/chapter-1-nis-risk-management-organisational-structures-andrequirements-v2.

[63] *Id*. at 4.

[64] *Id*. at 14.

[65] See *Eur. Comm'n, Internet of Things – An Action Plan for Europe* (June 18, 2009), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF.

[66] *A Cyber Security Framework For Europe*, *supra* note 61.

[67] *Id*.

[68] *Alliance for Internet of Things Innovation, Working Group 3 Report*, 2015. IoT LSP Standard Framework Concepts, Release 2.0, AIOTI WG03 – loT Standardisation.

[69] See *AIOTI News*, https://aioti.eu/news/ (last visited June 5, 2018).

[70] *Eur. Comm'n, Horizon 2020 Work Programme* (Oct. 13, 2015), http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/discussions/h2020-wp1617-focus_en.pdf.

[71] *Id*.

[72] *Id*. at 93.

[73] *Eur. Comm'n, Commission Priority, Digital Single Market, Bringing Down Barriers to Unlock Online Opportunities Digital Single Market*, http://ec.europa.eu/priorities/digital-single-market/index_en.htm.

[74] See "Framework for Improving Critical Infrastructure," 2015. *NIST*, at 4 (Apr.), http://www.nist.gov/cyberframework/upload/cybersecurity_framework_bsi_2015-04-08.pdf (noting that "To allow for adoption, Framework version 2.0 is not planned for the near term.").

[75] *DSM*, *supra* note 73.

[76] *Eur. Comm'n, An Environment Where Digital Networks and Services Can Prosper*, http://ec.europa.eu/priorities/digital-single-market/environment/index_en.htm (last visited Dec. 16, 2017).

[77] See, e.g., "Top Ten Operational Impacts of the GDPR," 2018. *Int'l Assoc. Privacy Prof.*, https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/ (last visited June 5).

[78] Scott Gordon, 2018. "Will we Get a GDPR for the IOT?," *SC Mag*. (Apr. 26), https://www.scmagazineuk.com/will-we-get-a-gdpr-for-the-iot/article/758037/.

[79] *Id*.

[80] Tim Turitto, "Achieving GDPR Compliance in Manufacturing," 2017. *Microsoft* (Dec. 15), https://cloudblogs.microsoft.com/industry-blog/industry/manufacturing/achieving-gdpr-compliance-in-manufacturing/.

[81] See Craig Guillot, 2017. "What American Manufacturers Need to Know about New Data Protection Laws in Europe," *Chief Executive* (May 31), https://chiefexecutive.net/american-manufacturers-need-know-new-data-protection-laws-europe/.

[82] Ian Wishart, 2015. "EU Strikes Cybersecurity Deal to Make Companies Boost Defenses," *Bloomberg* (Dec. 8), http://www.bloomberg.com/news/articles/2015-12-08/eu-strikes-cybersecurity-deal-to-make-companies-boost-defenses.

[83] "Cybersecurity Framework Frequently Asked Questions," http://www.nist.gov/cyberframework/cybersecurity-framework-faqs.cfm (last visited Sept. 21, 2015) ("Among other things, the EO directed NIST to work with industry leaders to develop the Framework. The Framework was developed in a year-long, collaborative process in which NIST served as a convener for industry, academia, and government stakeholders. That took place via workshops, extensive outreach and consultation, and a public comment process. NIST's future Framework role is reinforced by the Cybersecurity Enhancement Act of 2014 [Public Law 113-274], which calls on NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure. This collaboration continues as NIST works with stakeholders from across the country and around the world to raise awareness and encourage use of the Framework.").

[84] Shackelford, Russell, and Haut, *supra* note 60.

[85] Gordon, *supra* note 78.

[86] See, e.g., Arun Vishwanath, 2016. " 'Spearphishing' Roiled the Presidential Campaign – Here's how to Protect Yourself," *Conversation* (Nov. 8), https://theconversation.com/spearphishing-roiled-the-presidential-campaign-heres-how-to-protect-yourself-68274.

[87] See Andy Greenberg, 2016. "This 'Demonically Clever' Backdoor Hides in a Tiny Slice of a Computer Chip," *Wired* (June 1, https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/.

[88] See, e.g., Ian Baker, 2014. "The Global Supply Chain Behind the iPhone 6," *BetaNews*, https://betanews.com/2014/09/23/the-global-supply-chain-behind-the-iphone-6/.

[89] See Martin Giles, 2018. "Hackers Could Blow Up Factories Using Smartphone Apps," *MIT Tech. Rev.* (Jan. 11), https://www.technologyreview.com/s/609946/hackers-could-blow-up-factories-using-smartphone-apps/.

[90] See Ari Levy, 2016. "Amazon's Chinese Counterfeit Problem is Getting Worse," *CNBC* (July 8), https://www.cnbc.com/2016/07/08/amazons-chinese-counterfeit-problem-is-getting-worse.html.

[91] "Malware Being Installed on Computers in Supply Chain, Warns Microsoft", 2012. *Guardian* (Sept. 14), https://www.theguardian.com/technology/2012/sep/14/malware-installed-computers-factories-microsoft.

[92] See Elizabeth Weise, 2017. "FTC Settles with Lenovo Over a Built-In Snooping Software, $3.5 Million Fine," *USA Today* (Sept. 5), https://www.usatoday.com/story/tech/2017/09/05/ftc-settles-lenovo-over-built-snooping-software-scanned-users-computers/632775001/; Joshua A.T. Fairfield, 2017. "The 'Internet of Things' is Sending us Back to the Middle Ages," *Conversation* (Sept. 5), https://theconversation.com/the-internet-of-things-is-sending-us-back-to-the-middle-ages-81435.

[93] See Aaron Tilley, 2015. "How Hackers Could Use A Nest Thermostat As An Entry Point Into Your Home," *Forbes* (Mar. 6), https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#235d0d693986; Carl Franzen, 2017. "How to Find a Hack-Proof Baby Monitor," *Offspring* (Aug. 4), https://offspring.lifehacker.com/how-to-find-a-hack-proof-baby-monitor-1797534985; Charlie Osborne, 2015. "Smartwatch Security Fails to Impress: Top Devices Vulnerable to Cyberattack," *ZDNet* (July 22), http://www.zdnet.com/article/smartwatch-security-fails-to-impress-top-devices-vulnerable-to-cyberattack/; John Markoff, 2016. "Why Light Bulbs May B the Next Hacker Target," *N.Y. Times* (Nov. 3), https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r=0;

[94] "Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain," 2017. *IBM* (Mar. 5), https://www-03.ibm.com/press/us/en/pressrelease/51712.wss.

[95] Edmund Lee, 2016. "Why Blockchains can be Really Bad. Or: How Techno-Futurists can Ruin Things," *Recode* (June 19), https://www.recode.net/2016/6/19/11972818/dao-hacked-blockchain-ethereum.

[96] See Scott J. Shackelford and Steve Myers, 2017. "Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace," 19 *Yale J. L. & Tech.* 334.

[97] Monroe E. Price and Stefan G. Verhulst, 2005. *Self-Regulation and the Internet 21*. According to Notre Dame Professor Don Howard, different online communities "have a complicated topology and geography, with overlap, hierarchy, varying degrees of mutual isolation and mutual interaction. There are also communities of corporations or corporate persons, gangs of thieves, and . . . on scales small and large" (Don Howard, 2014. *Civic Virtue and Cybersecurity* 15, Working Paper). What is more, Professor Howard argues that these communities will each construct norms in their own ways, and at their own rates, but that this process has the potential to make positive progress toward addressing multifaceted issues such as enhancing cybersecurity. *Id.* at 22.

[98] See Price & Verhulst, *supra* note 97, at 21-22.

[99] Elinor Ostrom, 2008. *Polycentric Systems as One Approach for Solving Collective-Action Problems* 2–3 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08-6.

[100] "Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace," 2017. *Consumer Reports* (Mar. 6), https://www.consumerreports.org/media-room/press-releases/2017/03/consumer_reports_launches_digital_standard_to_safeguard_consumers_security_and_privacy_in_complex_marketplace/.

[101] "Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds," *Consumer Reports* (July 28, 2016), https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/.

[102] See Paul Hiebert, 2016. "Consumer Reports in the Age of the Amazon Review," *Atlantic* (Apr, 13), https://www.theatlantic.com/business/archive/2016/04/consumer-reports-in-the-age-of-the-amazon-review/477108/ ("More than 120 employees, with an annual testing budget of approximately $25 million, evaluate some 3,000 products a year. The results of these impartial studies are then gathered, examined, and published, ad-free, in *Consumer Reports*."); Allen St. John, 2018. "Europe's GDPR Brings Data Portability to U.S. Consumers," *Consumer Rep.* (May 25), https://www.consumerreports.org/privacy/gdpr-brings-data-portability-to-us-consumers/.

[103] Interview with Chris Palmer, Google engineer and former technology director, Electronic Frontiers Foundation, in San Francisco, Cal. (Feb. 25, 2011).

[104] Emily Stewart, 2015. "Cyber Attack Insurance Growing Fast," *ABC* (Oct. 9), http://www.abc.net.au/news/2015-10-09/cyber-attack-insurance-growing-fast/6842744.

[105] See id.; Nicole Perlroth, 2012. "Insurance Against Cyber Attacks Expected to Boom," *N.Y. Times Bits* (Dec. 29), http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/.; Robert Lemos, "Should SMBs Invest in Cyber Risk Insurance?," 2010. *Dark Reading* (Sept. 9), http://www.darkreading.com/smb-security/167901073/security/security-management/227400093/index.html; Jim Finkle, 2015. "Cyber Insurance Premiums Rocket After High-Profile Attacks," *Reuters* (Oct. 12), http://www.reuters.com/article/2015/10/12/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012.

[106] See Perlroth, *supra* note 105.

[107] But see Sarah Veysey, 2016. "Insurers Urge Anonymous Database to Help Underwrite Cyber Risks," *Bus. Insurance* (May 23), http://www.businessinsurance.com/article/20160523/NEWS06/160529961 ("The Association of British Insurers has called for a national anonymous database of cyber incidents to enable the insurance market to better assess, underwrite and price cyber risks).

[108] Finkle, *supra* note 105.

[109] See, e.g., Scott Shackelford, 2012. "Should Your Firm Invest in Cyber Risk Insurance?," 55 *Bus. Horizons* 349 (July-Aug.).

[110] See, e.g., 2015. "NIST Releases Draft Framework on the Internet of Things," *Hogan Lovells Chronicle of Data Protection* (Sept. 25), http://www.hldataprotection.com/2015/09/articles/consumer-privacy/nist-releases-draft-framework-on-the-internet-of-things/.

[111] Hogan Lovells, *supra* note 105.

[112] "NIST Releases Draft Framework to Help 'Cyber Physical Systems' Developers," 2015. *Nat'l Inst. Stan. & Tech.* (Sept. 18), http://www.nist.gov/el/nist-releases-draft-framework-cyber-physical-systems-developers.cfm.

[113] *Id.*

[114] NIST IoT Framework, *supra* note cx, at 12.

[115] *Id.* at 13.

[116] See Shackelford et al., *supra* note 39.

[117] IoT Cyber Bill Factsheet, https://www.warner.senate.gov/public/_cache/files/8/6/861d66b8-93bf-4c93-84d0-6bea67235047/8061BCEEBF4300EC702B4E894247D0E0.iot-cybesecurity-improvement-act---fact-sheet.pdf.

[118] *Id.*

[119] *Id.*

[120] See *New Bill Seeks Basic IoT Security Standards*, Krebs on Sec. (Aug. 1, 2017), https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/.

[121] See *S. 1691: Internet of Things (IoT) Cybersecurity Improvement Act of 2017 Track S. 1691*, https://www.govtrack.us/congress/bills/115/s1691 (last visited June 4, 2018).

[122] See Marguerite Reardon, *Senate Dems Introduce 'Privacy Bill of Rights*,' CNET (Apr. 10, 2018), https://www.cnet.com/news/senate-dems-introduce-privacy-bill-of-rights/.

[123] *Id.*

[124] See *As Facebook CEO Zuckerberg Testifies to Congress, Senators Markey and Blumenthal Introduce Privacy Bill of Rights*, Press Release Sen. Ed Markey (Apr. 10, 2018), https://www.markey.senate.gov/news/press-releases/as-facebook-ceo-zuckerberg-testifies-to-congress-senators-markey-and-blumenthal-introduce-privacy-bill-of-rights ("Specifically, the CONSENT Act: Requires edge

providers to obtain opt-in consent from users to use, share, or sell users' personal information; Requires edge providers to develop reasonable data security practices; Requires edge providers to notify users about all collection, use, and sharing of users' personal information; Requires edge providers to notify users in the event of a breach; Requirements are enforced by the FTC.").

[125] See Martin Matishak, *Lawmakers Gather Behind Election Security Bill — At Last*, Politico (Mar. 22, 2018), https://www.politico.com/story/2018/03/22/election-security-bill-congress-437472.

[126] See H.R.4036 - Active Cyber Defense Certainty Act, 115th Cong. (2017-2018), https://www.congress.gov/bill/115th-congress/house-bill/4036/actions.

[127] Nicholas Schmidle, 2018. "The Digital Vigilantes Who Hack Back," *New Yorker* (May 7), https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

[128] Josephine Wolff, 2017. "When Companies Get Hacked, Should They Be Allowed to Hack Back?," Atlantic (July 14), https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/.

[129] *Id.*

[130] *Id.*

[131] Schmidle, *supra* note 127.

[132] *Id.*

[133] *Id.*

[134] Wyatt Hoffman and Ariel Levite, 2017. "Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?," *Carnegie Cyber Pol'y Initiative* (June 14), http://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236.

[135] Michael D. McGinnis, 2011. "An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework," 39(1) *Pol'y Stud. J.* 163, 171–72 (Feb.), http://php.indiana.edu/~mcginnis/iad_guide.pdf (defining polycentricity as "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes.").

[136] Elinor Ostrom, 2008. *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08–6), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1.

[137] Elinor Ostrom, 2009. *A Polycentric Approach for Coping with Climate Change* 35 (World Bank, Policy Research Working Paper No. 5095), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.

[138] Robert O. Keohane and David G. Victor, 2011. "The Regime Complex for Climate Change*,"* 9 *Persp. on Pol.* 7, 9 *cf.* Julia Black, 2008. "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes," 2 *Reg. & Governance* 137, 157 (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees").

[139] See Martha Finnemore and Kathryn Sikkink, 1998. "International Norm Dynamics and Political Change," 52 *Int'l Org*. 887, 895–98 (1998).

[140] See Robert O. Keohane and David G. Victor, "The Regime Complex for Climate Change," 9 *Perspectives on Politics* 7 (2009)ns is not in that version. 10 points.ounting on you!nternational arbitrationplexity of futur 10 (Harvard Kennedy Sch., Discussion Paper 10-33, 2009) (internal quotation marks omitted), http://belfercenter.ksg.harvard.edu/files/Keohane_Victor_Final_2.pdf.

[141] For more on this topic, see Shackelford et al., "Toasters," *supra* note 6.

[142] Previously known as 'Information Systems Audit and Control Association,' http://www.isaca.org/about-isaca/Pages/default.aspx (last visited Dec. 16, 2015).

[143] "Existing Security Standards Do Not Sufficiently Address IoT," 2015. *IN Sec.* (Oct.), http://www.net-security.org/secworld.php?id=18981.

[144] See James Sanders, "Cybersecurity Tech Accord Sets New Privacy Standards for Tech Companies," 2018. *Tech. Rep.* (Apr. 18), https://www.techrepublic.com/article/cybersecurity-tech-accord-sets-new-privacy-standards-for-tech-companies/.

[145] See Adam Thierer, 2014. "Putting Privacy Concerns about the Internet of Things in Perspective," *Int'l Assoc. Privacy Prof.* (Feb. 3), https://iapp.org/news/a/putting-privacy-concerns-about-the-internet-of-things-in-perspective.

[146] See Paul M. Schwartz and Edward J. Janger, 2007. "Notification of Data Security Breaches," 105 *Mich. L. Rev.* 913, 922.

[147] These data have been compiled from the National Conference of State Legislature (NCSL) Report on Computer Crime Statutes, http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#Hacking (last updated June 14, 2018). It should also be noted that, in addition to these laws, 12 states maintain "data security laws," eight of which include a requirement for firms to implement "reasonable" cybersecurity practices. One example is Indiana. Ind. Code 24-4.9-3-3.5 ("A data base owner shall implement and maintain reasonable procedures, including taking any appropriate

corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner."). For more on this topic, see Jeff Kosseff, *Cybersecurity Law* 42-43 (2017). At least 31 states also boast data disposal laws that regulate when and how data is destroyed, including the use of "reasonable measures" to ensure that these data are "unreadable or undecipherable[.]" *Id.* at 49. Special thanks to Tristen Waite for her help in compiling these data.

Appendix A

Status of State-Level Cybersecurity Laws[147]

Type of State Law	Coverage	Description
Hacking, Unauthorized Access, Computer Trespass, Viruses, Malware	All 50 states	All 50 states have enacted laws that generally prohibit actions that interfere with computers, systems, programs, or networks.
Data Breach Notification Laws	All 50 states	
Anti-Phishing Laws	23 states: Alabama, Arkansas, Arizona, California, Connecticut, Florida, Georgia, Illinois, Kentucky, Louisiana, Michigan, Minnesota, Montana, New Mexico, New York, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia, Washington, and Guam	A total of 23 states and Guam have enacted laws targeting phishing schemes. Many other states have laws concerning deceptive practices or identity theft that may also apply to phishing crimes.
Anti-Denial of Service/DDoS Laws	25 states: Alabama, Arizona, Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Mississippi, Missouri, Nevada, New Hampshire, North Carolina, Ohio, Oklahoma, Pennsylvania, South Carolina, Tennessee, Virginia, Washington, West Virginia, and Wyoming	
Anti-Spyware Laws	20 states: Alaska, Arizona, Arkansas, California, Georgia, Hawaii, Illinois, Indiana, Iowa, Louisiana, Nevada, New Hampshire, New York, Pennsylvania, Rhode Island, Texas, Utah, Virginia, Washington, Wyoming, Guam, and Puerto Rico	There are 20 states and two U.S. territories have laws expressly prohibiting use of spyware. Other state laws against deceptive practices, identity theft, or computer crimes in general may be applicable to crimes involving spyware.
Anti-Ransomware Laws/ Computer Extortion Laws	5 states: California, Michigan, Connecticut, Texas, and Wyoming	Currently four states have statutes that address ransomware, or computer extortion; however, other state laws prohibiting malware and computer trespass may be used to prosecute these crimes as well.

Peer Reviewers: Jenifer Sunrise Winter, Associate Professor and Graduate Chair, School of Communications, University of Hawaii; Vishal Chawla, National Managing Principal, Risk Advisory Services, Grant Thornton; Chris Peters, CEO, The Lucrum Group; and David Chan, Consultant – ICS Cybersecurity Detection, Eli Lilly and Company

The Trade Impact of Smart Factories

Susan Ariel Aaronson*

Executive Summary

1. Smart factories will transform what's traded, how we trade, who trades, and when.
2. Smart factories link digital technologies (technologies built on data) with production processes.
3. In the wake of these changes, policymakers should update trade policies and agreements. Although trade agreements are written to be technologically neutral (not to favor specific technologies, and to be flexible enough to accommodate technological change over time), such agreements may not be clear or sufficient to address the changes posed by trade in data (which needs clarification) as well as the technologies that underpin smart manufacturing.

Overview

Entrepreneurs and executives have long tried to make workshops and factories smarter. For example, American industrial evolution in the 19th century is a history of how engineers, managers, and owners tried to diffuse new technologies such as the sewing machine, the reaper, the bicycle, and the automobile. Mechanics in these sectors who had learned how to create productive factories disseminated these ideas to other engineers, mechanics, and draftsmen, creating ever-more productive manufacturers (Hounshell 1984).

Today, entrepreneurs and executives continue that tradition, using data-based technologies to make their factories smarter. They use internet-connected devises or integrated circuits that enable sensing, measure, control, and communication to better manage workers, machines, and processes. By linking information technologies (modeling, big data, and artificial intelligence, etc.) with manufacturing technologies, these entrepreneurs and executives can meet rapidly changing global market needs in a timely basis.

Although smart manufacturing is not new, there is no official internationally accepted definition or terminology. The German and Chinese governments call smart manufacturing industry or factory 4.0—the fourth manufacturing age (Rüßmann et al. 2015). The U.S. government defines smart manufacturing as systems that are "fully-integrated, collaborative manufacturing systems that respond in real time to meet changing demands and conditions in the factory, in the supply network, and in customer needs" (NIST 2017). With smarter factories, firms can improve manufacturing efficiencies and enable managers and workers to make better decisions.

---

* *Susan Ariel Aaronson is Research Professor of International Affairs and GWU Cross-Disciplinary Fellow at the George Washington University's Elliott School of International Affairs.*

In 2013, China had the largest share of smart factories globally (18.8%), followed by Germany (15.1%), the USA (12.5%), Japan (13.3%), and Korea (11.3%) (Chang-do 2016, 26-27). However, some expect that the U.S. will displace China as the number one location for such factories by 2021 (Deloitte/Council on Competitiveness 2016).

This paper examines the impact of the technologies underpinning smart technologies upon trade. As Figure 1 shows, most of these technologies are built on gathering, manipulating, evaluating, and disseminating data.

With the advent of Cloud (and other data-driven) services, data in one country are increasingly stored, processed, and analyzed in another country. In this regard, data are essentially traded among individuals, firms, and states. Yet, there is no universal or even plurilateral system of rules to govern these cross-border data flows (Force Hill and Noyes 2018; de la Chappelle and Fehlinger 2016). Policymakers have yet to find common ground on how cross-border data should be controlled, priced, protected, and made secure. Without such agreement, data could deglobalize as growing numbers of states restrict the transfer of many types of data (Gupta and Fan 2018).

I argue that taken in sum, the technologies underpinning smart manufacturing could have two distinct and profound effects upon trade and trade rules. First, government efforts to foster smart factories could alter comparative advantage. In so doing, smart manufacturing will affect who trades what and when. Second, trade policymakers will also have to respond to the challenge of governing data and the technologies that underpin smart manufacturing (World Customs Organization 2017).

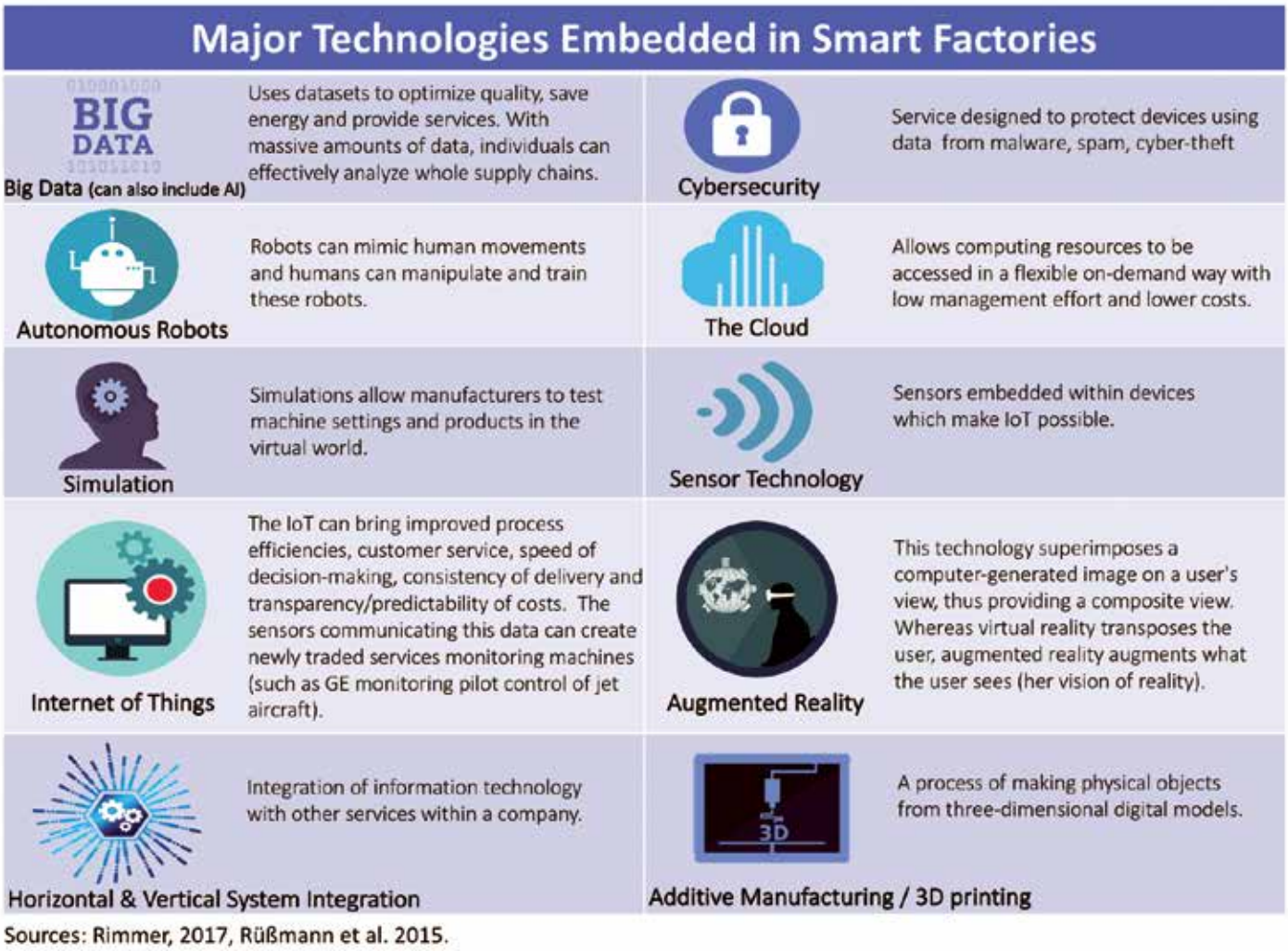

Figure 1. Major Technologies Embedded in Smart Factories. Graphic by Kailee Hilt.

The article proceeds as follows. I begin with some definitions. Next, I discuss how governments are trying to encourage smart manufacturing. I do not address how the technologies underpinning smart factories are leading to new types of relationships between individuals and firms or among firms. I note that it is an important component of the servicification of manufacturing (the growth of services affiliated with manufacturing). I then examine what trade rules say about smart factories and the technologies underpinning them. I next examine in depth two technologies that challenge current trade rules, 3-D printing and the Internet of Things (IoT). Finally, I develop some conclusions.

Definitions Used in this Overview

Smart factories merge and integrate production processes and digital technologies (digital devices, methods, and systems built on data) (Rüßmann et al. 2015, 4). Data and information (processed data) have long been a key component of trade, but recently data have created new forms of trade. Most trade agreements since the mid-1990s have included aspirational (non-binding) language governing e-commerce (goods and services delivered via the internet.) Digital trade is a broader term that not only includes e-commerce, but also rules to govern services delivered via the internet and associated technologies (such as cloud computing, apps, and voice-over-internet calls).

Government Efforts to Achieve Comparative Advantage in Smart Manufacturing

Policymakers in many countries understand that they must invest in smart manufacturing technologies if they want to maintain a strong manufacturing sector (World Economic Forum and McKinsey 2018; Ezell 2016). Government officials can foster these sectors with tactics including funding research and development, using the tax code to stimulate types of investment, creating an effective enabling environment for diffusion of smart manufacturing, encouraging worker training, and using trade agreements to ensure market access (Leiva 2017; Ezell 2016 and 2018; World Economic Forum and McKinsey 2018). For example, the German government has encouraged multi-sectoral collaboration to build smart factories since 2011. Germany has a strong head start because of its cooperative approach to manufacturing, focus on precision engineering, and ability to disseminate new ideas and processes (Germany Trade and Investment 2018; Bonvillian 2016).

In contrast, the Chinese government is both a demandeur, a catalyst, and a venture capitalist for smart manufacturing. Smart factories are also a major focus of China's plan to facilitate modernization and diversification of the Chinese economy based on innovation. The *Made in China 2025* plan unveiled by Premier Li Keqiang in 2015 provides government support for the development of smart manufacturing technologies such as 3D printing, big data analytics, and robotics.[1] Li aims to transform China into a "strong" manufacturing nation in a decade, and match the strengths of Germany and Japan as leading innovators in certain industries within two decades. China also has some real advantages because it has the world's largest manufacturing base (Chang-do 2016).

The U.S. has also been trying to stimulate advance manufacturing using the power of government to convene, disseminate, and invest in smart manufacturing. A catalyst for U.S. government action was a significant drop in manufacturing employment. Between 2000 and 2010, U.S. manufacturing employment fell by 5.8 million jobs, from 17.3 million to 11.5 million in 2015. Such jobs were an important route to the middle class for many Americans without college degrees, and the loss of these engendered significant social and economic upheaval in towns where plants left (Bonvillian 2016).

Influenced by a series of key academic reports, recommendations from two presidential task forces, and a 2012 national strategic plan for advanced manufacturing, Congress enacted legislation in 2014 to address the issue. The Reinventing American Manufacturing and Innovation (RAMI) Act established Manufacturing USA, a federal program to support government-industry-academic collaboration to bridge the so-called "valley of death" in precompetitive technologies.

These national efforts all aim to spur innovation in smart manufacturing or advanced manufacturing. However, the OECD argues that policymakers should also create "effective institutions dedicated to technology." Moreover, because data is an essential element of smart manufacturing, a unified approach to data and data openness, protection, and rules for sharing and control will be essential. Most states have yet to develop national data plans, yet data, as the OECD notes, needs "to be treated as a new infrastructure for 21st century production" (OECD 2016, 3-4).

Table 1 summarizes the efforts of some nations to achieve comparative advantage in this new sector.

Industrialized country officials may see smart manufacturing as a way to wed their digital expertise with longstanding management skills. They may hope that this linkage will bring manufacturing "back" to higher wage nations. They also hope to build new markets for customized and precision manufactured goods. On one hand, their hopes may be granted. According to technology analyst Steven Ezell, smart manufacturing "can lower labor costs relative to total costs," so it could make at-the-margin manufacturing easier to locate in higher-cost areas. But African, Chinese, Indian, and other countries may find strategies that allow them to compete equally well for such firms with low-cost loans or lower real estate prices or subsidized infrastructure. At the same time, smart manufacturers will require higher-skilled workers on the shop floor, making it problematic for low-wage nations, where potential workers have limited skills. Finally, by reducing efficient minimum production scale, in part through customized manufacturing, smart manufacturing will make it more economically feasible to locate some work closer to the customer base, and that will often be in higher-income nations" (Ezell 2016, 22).

However, the belief that western democracies with unionized workers may dominate smart manufacturing may be overly optimistic. Few democracies can push forward with long-term industrial planning without significant debate. Moreover, their citizens could be negatively affected by changes that could affect their jobs, income, and social/political views. Although executives will decide whether to invest, government policies and subsidies could play a deciding role in their decision-making process. In contrast with authoritarian states, citizens and policymakers alike may be reluctant to subsidize technologies that they fear could lead to economic and social upheaval. U.S. history shows that sectors experiencing rapid improvements in productivity can increase output with fewer workers and lead to a rapid decline in sector employment (e.g., the agricultural sector from 1900-1930).

Trade Rules Governing Smart Factories

There are no trade rules governing smart factories per se. The most multilateral trade agreement, the World Trade Organization (WTO) and most bilateral or regional trade agreements predate the invention of many of the technologies that underpin smart factories. Nonetheless, the WTO includes several agreements that govern trade in the goods and services produced by and essential to creating smart factories. These agreements include the Information Technology Agreement (ITA), which eliminates duties for trade in digital products; the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs), which protects trade-related intellectual property pertinent to information technology; and the General Agreement on Trade in Services (GATS), which has chapters on financial services, telecommunications, and e-commerce that relate to cross-border data flows (Aaronson 2018). Member states have also agreed not to tax electronic transmissions that flow across borders (ICTSD 2017). These rules not only say what governments can and can't do regarding trade, but they also delineate how and when nations can breach these rules. Under the exceptions, signatory nations can restrict trade in goods, services, and data in the interest of protecting public health, public morals, privacy, national security, or intellectual property, so long as such restrictions are necessary and proportionate and do not discriminate among the 164 WTO member states (Goldsmith and Wu 2006).

Member states designed the GATS language to ensure it would remain relevant as technology changed, but several member states have said that they need clarification on specific points and want to update these rules to

Table 1. Summary of National Smart Manufacturing Policies / Programs by Country

Country	Smart Manufacturing Policy / Program	Investment Level
Canada	The "Strategic Innovation Fund" will consolidate and simplify innovative programming for various areas, including: a) Strategic Aerospace and Defense Initiative b) Technology Demonstration Program c) Automotive Innovation Fund d) Automotive Supplier Innovation Program It will encourage research and development, accelerate technology transfer and commercialization of innovative products, processes and services; facilitate expansion of firms; attract large scale investments; advance the development of technology through collaboration with academia, non-profit organizations, and private sectors.	The 2017 budget proposed 1.26 billion dollars over five-years, which will allocate repayable and non-repayable contributions to firms of all sizes across Canada's industrial and technology sectors.
China	The "Made in China 2025" is an action plan to promote the development of Chinese service-oriented manufacturing. The plan highlights 10 priority sectors relevant to smart manufacturing including: a) New advanced information technology b) Automated machine tools & robotics c) Maritime equipment and high-tech shipping d) Modern rail transport equipment e) New energy vehicles and equipment f) Power equipment g) New materials h) Advanced medical products The plan also foresees the creation of 15 manufacturing innovation centers by 2020 and 40 by 2025.	The program was issued in 2015 and did not include a specific funding line; however, China invested 20 billion yuan (3.05 billion U.S. dollars) in "advanced manufacturing" in 2016.
France	Industrie du Futur aims to make France a leader in the world's industrial renewal by bringing together professional organizations from industry and digital technology along with academic and technological partners. The main areas of the plan are: a) Ecological transition b) Vocational training c) Innovation d) Digital transformation of the public services	Starting in 2015 the government will invest €57 billion over 5 years.
Germany	Industrie 4.0 was implemented by the Ministry of Education and Research and the Ministry for Economic Affairs and Energy. It refers to the national and international activities that surround digital transformation in Germany. The platform unites stakeholders from various economic sectors, professional associations, scientific communities, trade unions, and government departments to collaborate on innovative strategies. The work of the platform consists of 4 concentrated areas: a) Making content recommendations b) Providing single source support c) Promoting international networking d) Mobilizing businesses -particularly small and medium sized enterprises	Funding of up to €200 million has been provided by the government, followed by €120 given by Ministry of Education and Research, and €80 given by Ministry for Economic Affairs and Energy.

Sweden	The "Smart Industries" strategy for new industrialization will strengthen companies' capacity for change and competitiveness in a shifting landscape for manufacturing and production. The plan includes 4 focus areas: a) Industry 4.0 b) Sustainable Production c) Industrial Skills Boost d) Test Bed Sweden	The strategy will invest 11.5 million SEK (1.24 million U.S. dollars, the project is to be reviewed in March 2020).
United Kingdom	The "Industrial Strategy" launched in 2017 seeks to create an economy that will increase productivity and earning power through the foundation of ideas, people, infrastructure, business environment, and places. Specifically, the Office for AI will work initially with six priority business sectors: cybersecurity; life sciences; construction; manufacturing; energy; and agricultural technology to find ways to boost productivity through artificial intelligence and data analytic technologies. In partnership with industry experts and academia, these bodies will foster research and innovation, stimulate demand and accelerate uptake across all sectors of the economy.	It will invest £725m in new Industrial Strategy Challenge Fund programs to capture the value of innovation.
United States	Inspired by the success of Germany's famed Fraunhofer Institutes, Manufacturing USA currently comprises 14 institutes that are geographically dispersed. Each institute focuses on a core set of related technologies. The program has four stated goals: (1) To increase the competitiveness of U.S. manufacturing; (2) facilitate the transition of innovative technologies into scalable, cost-effective, and high performing domestic manufacturing capabilities; (3) accelerate the development of an advanced manufacturing workforce; and (4) support business models that help institutes to become stable and sustainable after the initial federal startup funding period.	Federal funds are authorized for a five-year period. The federal funding level is typically $70-110M per institute, matched or exceeded by funding from private industry and other non-federal sources, with a minimum 1:1 cost share. To date, the federal-nonfederal ratio exceeds 1:2.

Sources: Kennedy 2015; European Commission 2017; France Ministry for the Economy and Finance 2018; Government of Canada 2018; Government Offices of Sweden 2016; HM Government;2017.

Prepared by: Kailee Hilt

avoid misunderstanding. In 1998, members agreed not to put customs duties on electronic transmissions, as noted earlier. However, since then they have made little progress. They have tried to delineate rules to govern e-commerce (goods and services delivered online) and trade in computer or digital services through a new agreement called the Trade in Services Agreement (TiSA). But they have not yet found consensus.

The GATS has two sets of exceptions when nations can breach these rules: the General Exceptions and the National Security Exception. Under these exceptions, signatory nations can restrict trade in the interest of protecting public health, public morals, privacy, national security, or intellectual property, as long as such restrictions are necessary and proportionate and do not discriminate among WTO member states. There is no consumer protection exception. Moreover, WTO dispute settlement bodies have found that "measures must be applied in a manner that does not constitute arbitrary or unjustifiable discrimination or a disguised restriction on trade in services." Finally, countries should ensure that they use these exceptions in a reasonable manner so as not to frustrate the rights that they have accorded to other members (Goldsmith and Wu 2006).

Meanwhile, although the GATS states nothing explicitly about data flows, WTO members have begun to apply these obligations when settling disputes about cross-border data flows (Wunsch-Vincent 2006; Goldsmith and Wu 2006). The WTO Dispute Settlement Body has adjudicated two trade disputes related to data flows. These disputes have provided some insights into when and how nations can use the exceptions and clarified that the GATS apply to new computer services including e-commerce or 3-D printing.

In the absence of negotiating progress at the WTO, the United States, EU, Canada, and other nations have been actively pursuing bilateral and regional free trade agreements. For example, the Comprehensive and Progressive Trans-Pacific Partnership (CP-TPP) is a trade agreement among 11 nations bordering the Pacific including Japan, Australia, Canada, Mexico, Chile, and Malaysia. (The U.S. was a signatory, but President Trump withdrew the U.S. from the agreement in 2017). CP-TPP includes language making the free flow of data a default; it bans requirements to locate data only in local servers; and bans requirements to divulge computer source code (e.g., algorithms). However, it also includes a wide berth of exceptions (Aaronson 2018, forthcoming). NAFTA 2.0 (now the USMCA) also includes digital trade provisions including stronger language on privacy. As of this writing, no such regional agreement with binding language on data flows has come into effect. Moreover, because they are regional rather than universal, these agreements could further fragment the internet, raising costs for businesses that rely on cross-border data flows.

Finally, the three largest producers and markets for data, the U.S., the European Union, and China, are using domestic and foreign policies to reap data-based economies of scale and scope. Essentially, they have created three distinct data realms with different approaches to data governance (Aaronson and LeBlond 2018). In the U.S. realm, policymakers have put few limits on cross-border data flows. They use trade agreements to develop economies of scale and scope in data and to ban practices such as data and server localization requirements, which could distort trade as well as undermine U.S. comparative advantage in data-driven sectors. In contrast, the EU has made personal data protection the top priority for its realm, in the belief that it will build trust and help netizens feel more comfortable as firms use their personal data. Finally, policymakers in the Chinese realm restrict the free flow of data and information both within China and between China and other nations. In so doing, Chinese officials maintain social stability and the power of the Communist Party, while simultaneously nurturing knowledge-based sectors such as artificial intelligence (Aaronson and LeBlond 2018).

The data-driven economy is not yet a global phenomenon. Many countries are putting in place plans to facilitate the development of data-driven sectors. Figure 2 provides an overview estimation of these activities.

How Smart Manufacturing Technologies Will Change Trade Policies

Table 2 describes some technologies that underpin smart factories and how they may affect existing trade rules. As the table illustrates, some of the technologies embedded in smart manufacturing will need clarification under existing trade rules. Others will require brand new trade rules to effectively regulate how they may affect trade.

Two Issues in Depth: 3-D printing and the IoT

3-D printing refers to a manufacturing process in which a material is joined or solidified under computer control to create a multi-dimensional object based on a digital model (such as a 3-D model or one build through computer aided design). 3-D printing will make it easier to customize products for specific consumers, facilitating more localized supply chains.

3-D printing will have mixed effects on trade. If demand falls for one product one quarter, a company can easily adjust its output to products or locations where there is greater demand, facilitating trade (D'Aveni 2018). But 3-D printing may also act as a disincentive to trade. The Dutch Bank ING argues that world trade will shrink by 23% in 2060 if investments in 3-D printers continue at the current pace. The Bank also forecast that 3-D printing

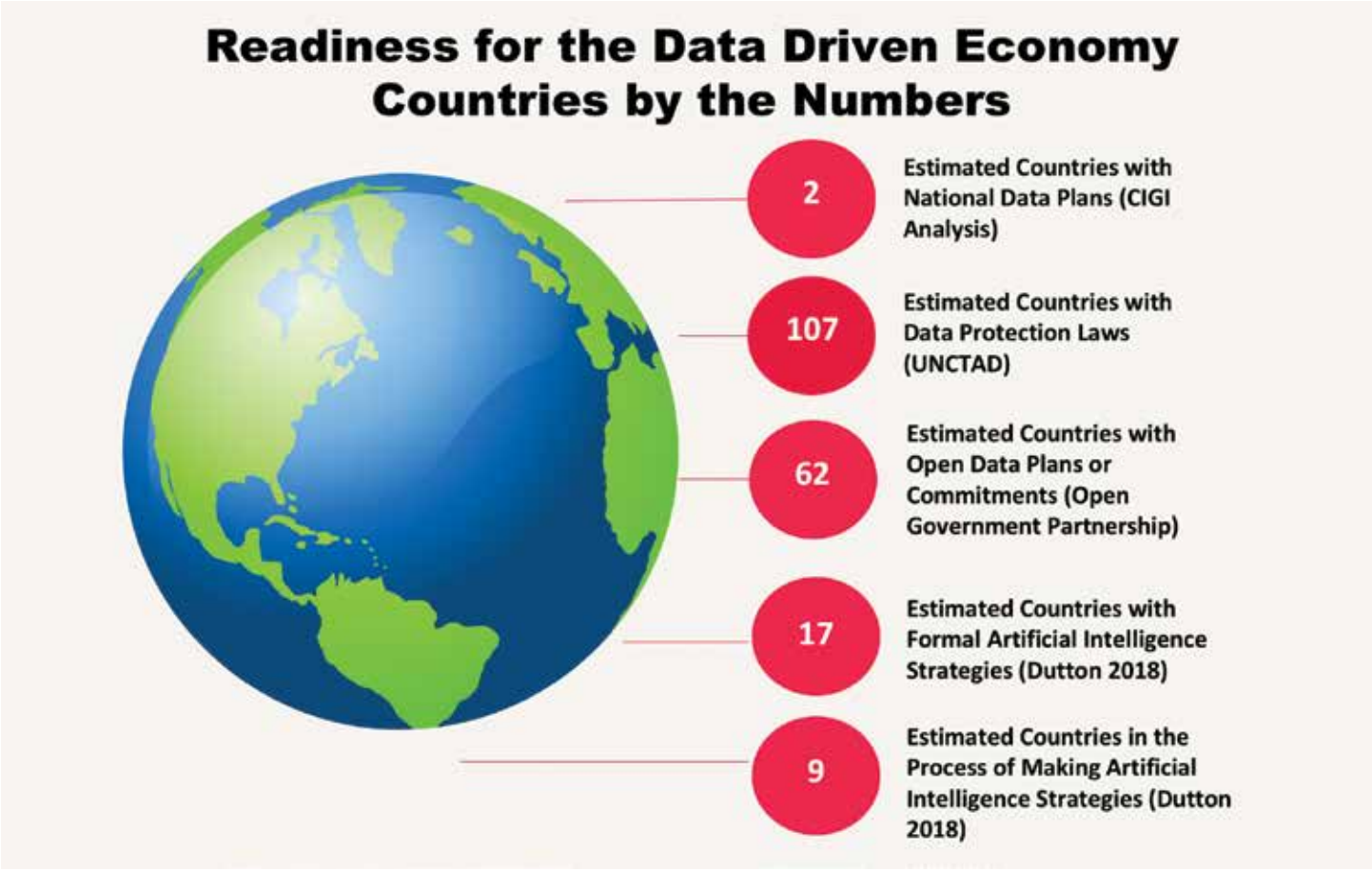

Figure 2. Readiness for the Data Driven Economy; Countries by the Numbers. Graphic by Kailee Hilt.

will reduce U.S. trade deficits with Mexico and Germany (automotive) and China (machines, consumer products) (ING 2017, 3).

3-D printing will challenge trade policymakers in several ways, including:

- Making trade agreements less relevant because trade will be less essential to firms.
- Undermining trade norms of non-discrimination between goods made in traditional factories and goods made through 3-D printing.
- Elevating and expanding services embedded in manufacturing as more companies attempt to create personalized products linked to such services (as example, embedded sensors for heart problems and services monitoring those sensors).
- Furthering regulatory competition regarding intellectual property. Firms might choose to locate in a specific country with stronger or more lax regulation in of 3-D printing for information technology, medicine and biotechnology (Kommerzcollegium 2016).
- Furthering competition about how best to promote innovation-open sharing of plans and process vs. the more closed proprietary protection of knowledge and technologies (World Intellectual Property Organization-WIPO 2015).
- Prodding policymakers to rethink rules of origin (where a product was made) and valuation (how a product is valued for customs purposes).
- Prodding policymakers to rethink what is a good, given that such much of a 3D printed good is data and associated services (World Customs Organization 2016).

Table 2: Some of the Technologies Embedded in Smart Manufacturing and their Implications for Trade

Type of technology	Issues relevant to trade rules	Covered? Areas of clarification?	Need new rules?
Big data and analytics (including AI)	Treatment of cross-border data flows	Covered in WTO, established through trade disputes, but language is implicit.	Yes. Will need rules regarding application that have governance implications (e.g. disinformation and national security, stability, rules governing exceptions, privacy
Internet of Things	Security and privacy (data protection issues)	Covered but bi-dimensional which could yield confusion and trade disputes. IoT=Data/ services bunded in a good. Goods covered under GATT, services under GATS	Need clarity given different national approaches to national security, social stability and privacy/data protection. Raises questions for services where a nation has not made a commitment. IPR, valuation issues. May need new rules.
Cybersecurity	National security implications covered, but unclear. Not directly addressed in trade rules	Has become a trade issue justified under the exceptions. Some FTAs include cooperative language	Need clearer rules as to when nations can use cybersecurity to justify an exception re. GATS/GATT. No common norms regarding how to keep information secure and when governments can restrict data flows (censorship) to keep internet secure
The Cloud	Leading to many trade debates re. privacy and national security	Incomplete and unclear	Will need clarification regarding when national jurisdiction ends, and clarification of exceptions for privacy and national security.
Additive manufacturing/3-D printing	Policymakers are just beginning to address trade implications	Incomplete and unclear	Raises customs, rules of origin, valuation, and copyright issues. Could expand product differentiation and complicate definitions of "like product" (is a 3-D printed item the same as a manufactured item?) May need new rules.

Sources: Aaronson: 2018, Chander: 2015, Rimmer: 2017, WTO: 2018 (forthcoming) and 2017.

The IoT enables advanced services by interconnecting (physical and virtual) things to identify, sense, network, and process data. Like 3-D printing, the IoT will have mixed effects on trade. It could improve shipping and transport efficiencies (Lund and Manyika 2016 and *The Economist* 2018). But it could also lead to a trade bottleneck. Nations with greater research capabilities in the IoT, data analytics, and computing could enjoy first-mover advantages from the digitalization of industry, but populous countries rich in data could also use their data pools as leverage over such firms. These states could demand new models of compensation for data holders or new models of regulation of data to obtain market access (Aaronson and LeBlon 2018).

The IoT challenges trade policymakers in several ways, including:

- Making services affiliated with goods more important to trade;
- Forcing a rethink of valuation given the import of embedded services (Chander 2015, 8);
- Prodding policymakers to make personal data protection and data security a priority and clarify trade rules related to privacy. Consumers won't trust the IoT unless they know their data will be protected. However, nations must rely on the privacy exception if they want to maintain personal data in local servers (Aaronson 2018a; Chander 2015; CIGI-Ipsos 2018). Yet some see privacy regulations as a trade barrier (Gupta and Fan 2018). The IoT and data protection can be reconciled. The U.S., EU, Mexico, and Canada have agreed to trade rules that ban data localization except under the exceptions in the EU/Mexico FTA and USMCA. Privacy is a legitimate exception as noted above. The EU requires its trade partners to be found adequate to exchange personal data across borders. (These agreements are not yet in effect.[2]) This raises important security and cybersecurity questions for governments related to computers, telecommunications, and cloud-related procurement (Finley 2018). Many countries justify procurement rules that require certain types of data to be stored locally or requiring the purchase of certain types of products for national security reasons. Policymakers struggle to determine legitimate privacy and national security needs vs. trade distorting practices (Aaronson 2018a).

Rules Governing Data Need to Be Updated and Clarified

The technologies underpinning smart factories are built on significant amounts of data. Executives and entrepreneurs need to obtain this data from many different countries; these countries with have different regulations regarding the use of technologies and personal data. This creates a catch-22. Smart factories need global access to data to achieve economies of scale and scope. Firms that can achieve economies of scale using data can decrease the costs of production of a good or service; economies of scope allow a firm to produce many different types of products to reduce costs. Policymakers in many countries want to encourage these scale economies with shared norms, rules, and exceptions to these rules. In developing these exceptions, these officials want to limit trade in some types of data to ensure the safety and privacy of their citizens. Hence, policymakers must devise a new approach to regulating trade in data because so much of this data is personal data.

To accomplish this aim, trade diplomats and internet policymakers could call for an international meeting to establish an interoperable approach to data protection and control which allows nations to evolve their own complementary approaches and make them interoperable. The meeting should be attended by a diverse set of individuals, firms and agencies involved in privacy and data protection issues, and it should be tasked to build on existing principles such as the APEC and OECD Privacy Principles. Companies and data protection officials have already found some common ground on helping companies that move data globally transcend different regulatory strategies (Carson 2014 and 2015). But there seems to be a growing sense that the U.S. approach is too focused on ensuring that personal data can be utilized as a commercial asset, while the EU has put the suppliers of personal data first. The organizers should establish a web site that will be "marketed" by participating governments. The architects of the site will ask netizens to crowd-source ideas about how to build on these existing principles while simultaneously empowering people to control their personal data (World Economic Forum 2011).

Conclusion

Professor Mark Lemley of Stanford Law School warned that the internet has introduced a raft of new technologies that separate creativity from production and distribution and reduce the cost of all three activities. The technologies "challenge the basis for our economy as a whole" (Lemley 2015, 515). Lemley is right: Smart factories include many technologies that are changing how and what we produce and how we think about the relationship between products and associated services. Trade policymakers have a responsibility to ensure that

the system of rules governing trade in both the data and technologies underpinning smart factories are governed in a transparent, accountable, and trusted manner. It won't be easy.

References

Aaronson, Susan Ariel, 2018a. "What are We Talking About When We Talk about Digital Protectionism?" *World Trade Review*, Summer, 1-37.

Aaronson, Susan Ariel and Patrick LeBlond, 2018. "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO," *Journal of International Economic Law*, https://doi.org/10.1093/jiel/jgy019.

Bonvillian, William, 2016. OECD: "Smart Industry: Enabling the Next Production Revolution," November 17, http://www.oecd.org/sti/ind/Bonvillian.pdf.

Carson, Angelique, 2014. "European Regulators, FTC Unveil Cross-Border Data Transfer Tool," *IAPP News*, March 4, https://iapp.org/news/a/european-regulators-ftc-unveil-cross-border-data-transfer-tool/.

Carson, Angelique, 2015. "EU and APEC Officials Agree to Streamline BCR/CBPR Application Process," *IAPP News*, May 26, https://iapp.org/news/a/eu-and-apec-officials-agree-to-streamline-bcrcbpr-application-process/.

Chang-do, Kim, 2016. "China is Shifting to the "Smart Factory of the World," Posco Research Institute, Vol. 02, October, https://www.posri.re.kr/files/file_pdf/59/329/6681/59_329_6681_file_pdf_1476086212.pdf.

Chander, Anupam, 2015. "Robots, the Internet of Things, and the Future of Trade," October 23. UC Davis Legal Studies Research Paper No. 465. Available at SSRN: https://ssrn.com/abstract=2679028 or http://dx.doi.org/10.2139/ssrn.2679028.

Centre for International Governance Innovation (CIGI) and Ipsos, 2018. 2018 CIGI-Ipsos Global Survey on Internet Security and Trust, https://www.cigionline.org/internet-survey-2018.

D'Aveni, Richard A., 2018. "Five Myths, 3-D Printing," *Washington Post*, August 12, https://www.washingtonpost.com/outlook/five-myths/five-myths-about-3-d-printing/2018/08/10/9cb583fe-9c18-11e8-b60b-1c897f17e185_story.html?utm_term=.c5c6d052ee41.

de La Chappelle, Bertrand and Paul Fehlinger, 2016. "Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation", 28 Centre for International Governance Innovation Papers, https://goo.gl/o9tNRT.

Deloitte/Council on Competitiveness, 2016. *Global Manufacturing Competitiveness Index*, https://www2.deloitte.com/global/en/pages/manufacturing/articles/global-manufacturing-competitiveness-index.html.

Ezell, Steven, 2016. *A Policymaker's Guide to Smart Manufacturing, Information Technology and Innovation Foundation*, http://www2.itif.org/2016-policymakers-guide-smart-manufacturing.pdf.

Ezell, Steven, 2018. *Why Manufacturing Digitalization Matters and How Countries Are Supporting It*, April, http://www2.itif.org/2018-manufacturing-digitalization.pdf.

Finley, Clint, 2018. Australia's Ban on Huawei Is Just More Bad News for China, Wired, August 24, https://www.wired.com/story/australias-ban-on-huawei-is-just-more-bad-news-for-china/

Force Hill, Jonah and Matthew Noyes, 2018. "Rethinking Data, Geography, and Jurisdiction: Towards a Common Framework for Harmonizing Global Data Flow Controls," in Ryan Ellis and Vivek Mohan (Eds.), *Rewired: Cybersecurity Governance*. Wiley Publishing. https://goo.gl/FwuLcB.

Germany, Trade and Investment, *INDUSTRIE 4.0*, https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Why-germany/industrie-4-0-why-germany-actors.html; and https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Industrie-4-0/industrie-4-0-what-is-it.html.

Goldsmith, Jack and Tim Wu, 2006. *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.

Gupta, Anil and Ziyang Fan, 2018. "The Dangers of Digital Protectionism," *Harvard Business Review*, August 30, https://hbr.org/2018/08/the-dangers-of-digital-protectionism.

Hounshell, David A., 1984. *From the American System to Mass Production*, 1800-1932., Baltimore: Johns Hopkins.

International Centre for Trade and Sustainable Development (ICTSD), 2017. "African Group Submits Proposal on E-commerce Ahead of WTO Ministerial," 28 November, https://www.ictsd.org/bridges-news/bridges-africa/news/african-group-submits-proposal-on-e-commerce-ahead-of-wto.

ING, 2017. 3-D *Printing: A Threat to Global Trade*, September, https://www.ingwb.com/media/2088633/3d-printing-report-031017.pdf.

Kennedy, Scott, 2015. *Made in China 2025*. Center for Strategic and International Studies. https://www.csis.org/analysis/made-china-2025.

Kommerskollegium, 2016. *Trade Regulation in a 3D Printed World – a Primer*, Swedish National Board of Trade.

Leiva, Conrad, 2017. "The Role of Government in Manufacturing Infrastructure Support," October 4, https://mfgday.industryweek.com/2017/10/04/the-role-of-government-in-manufacturing-infrastructure-support/.

Lemley, Mark, 2014. "IP in a World Without Scarcity," *NYU Law Review*, May Volume 90, Number 2, http://www.nyulawreview.org/issues/volume-90-number-2/ip-world-without-scarcity.

Lund, S. and J. Manyika, 2016. *How Digital Trade is Transforming Globalisation,* Geneva: ICTSD and WEF.

NIST, 2017. "Smart Manufacturing," www.nist.gov/topics/smart-manufacturing.

Organization for Economic Cooperation and Development (OECD) "Enabling the Next Production Revolution: The Future of Manufacturing and Services, Interim Report, June1-2, 2016, https://www.oecd.org/mcm/documents/Enabling-the-next-production-revolution-the-future-of-manufacturing-and-services-interim-report.pdf.

Rimmer, Matthew, 2017. "The Maker Movement: Copyright law, Remix Culture and 3D printing," The University of Western Australia *Law Review* 41(2): 51-84, https://ssrn.com/abstract=2910832.

Rüßmann, Michael, Markus Lorenz, Philipp Gerbert, Manuela Waldner, Jan Justus, Pascal Engel, and Michael Harnisch, 2015. "Industry 4.0, The Future of Productivity and Growth in Manufacturing Industries," Boston Consulting Group, April, https://www.zvw.de/media.media.72e472fb-1698-4a15-8858-344351c8902f.original.pdf.

The Economist, 2018a. "How AI is spreading throughout the supply chain," Special report, *In Algorithms We Trust*, print edition, 31 March 2018.

Thomas, Juan Pedro, 2018. "Siemens to build smart manufacturing center in China," *South China Morning Post*, January 18, https://enterpriseiotinsights.com/20180118/smart-factory/siemens-build-smart-manufacturing-center-china-tag23.

World Customs Organization, 2017. "WCO ITC concludes with expert insights on the Power of Data," June 16, http://www.wcoomd.org/en/media/newsroom/2017/june/2017-wco-itc-concludes-with-expert-insights-on-the-power-of-data.aspx.

World Economic Forum and McKinsey, 2018. "The Next Economic Growth Engine: Scaling Fourth Industrial Revolution Technologies in Production," *World Economic Forum*, January, http://www3.weforum.org/docs/WEF_Technology_and_Innovation_The_Next_Economic_Growth_Engine.pdf.

World Intellectual Property Organization (WIPO), 2015. *World IP Report: Breakthrough Innovation and Economic Growth*, http://www.wipo.int/edocs/pubdocs/en/wipo_pub_944_2015.pdf.

World Trade Organization (WTO), 2018 (forthcoming), *World Trade Report* (draft in possession of author).

World Trade Organization (WTO), 2017, *World Trade Report, Trade Technology, and Jobs*, https://www.wto.org/english/res_e/publications_e/wtr17_e.htm.

Websites

GATS Exceptions

WTO Analytical Index, www.wto.org/english/res_e/publications_e/ai17_e/ai17_e.htm.

For Table 2

European Commission, 2017. Digital Transformation Monitor: France Industrie du Futur. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%20du%20Futur%20v1.pdf.

European Commission, 2017. Digital Transformation Monitor: Germany Industrie 4.0. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%204.0.pdf.

France Ministry for the Economy and Finance, 2018. New Industrial France. https://www.economie.gouv.fr/files/files/PDF/web-dp-indus-ang.pdf.

Government of Canada, 2018. "Strategic Innovation Fund," Innovation, Science and Economic Development Canada. http://www.ic.gc.ca/eic/site/125.nsf/eng/home.

Government Offices of Sweden, 2016. Smart industry – a strategy for new industrialization for Sweden. https://www.government.se/498615/contentassets/3be3b6421c034b038dae4a7ad75f2f54/nist_statsformat_160420_eng_webb.pdf.

HM Government, 2017. "Industrial Strategy: Building a Britain fit for the future," Industrial Strategy White Paper, https://www.timeshighereducation.com/sites/default/files/breaking_news_files/industrial-strategy-white-paper.pdf.

Endnotes

[1] *Made in China 2025* has nine goals: (1) enhancing innovation capability and boosting innovation in manufacturing; (2) promoting the integration of industrialization and IT (e.g., promoting digitalization); (3) strengthening the fundamental capacity of industry in basic components, basic processing technologies, basic materials, and basic industrial services; (4) boosting the quality and recognition of Chinese brands; (5) making Chinese manufacturing practices greener; (6) targeting priority technologies and products; (7) restructuring industry; (8) developing manufacturing as a service vice and services for manufacturing; and (9) identifying opportunities for international collaboration. Ezell: 2018,34.

[2] See Digital Trade Chapter EU/Mexico http://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf and for NAFTA. It contains a review clause that the EU finalized in July 2018; see http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157129.pdf. For the digital trade provisions in NAFTA 2.0, see https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/19%20Digital%20Trade.pdf.

Peer Reviewers: Lisa Schroeter, Global Director of Trade and Investment Policy, The Dow Chemical Company and Wilfred Mascarenhas, Advisor—Data & Analytics, Manufacturing and Quality IT, Eli Lilly and Company.

Challenges and Opportunities

Keith B. Belton

Manufacturing firms are not monolithic; they differ significantly in the products they produce, the inputs they employ to make these products, their upstream suppliers and their downstream customers, their relative size (e.g., in terms of employees or annual revenue), and the processes that transform these inputs into finished goods.

Manufacturers also share certain characteristics. Most serve other manufacturers (B2B) as opposed to end-use consumers (B2C); all manage both operations technology (OT) as well as information technology (IT); production assets often last decades prior to replacement; production downtime is extremely costly and to be avoided if possible; supply chains are increasingly complex in terms of the sheer number and locations of suppliers and customers; and rapidly evolving technology increases demand for employees with a new set of skills.

Might these similarities and differences help explain the major challenges and opportunities faced by manufacturers wishing to create and/or invest in smart factories? To find out, the Manufacturing Policy Initiative (MPI) at Indiana University invited executives from 18 manufacturing firms to Washington, D.C., to engage in a facilitated discussion on smart manufacturing, with a focus on information governance issues. In preparation for this meeting, the executives (see the Appendix A for a list of participants) were given the preceding papers on artificial intelligence, technical standards, cybersecurity/privacy, and digital trade.

During the meeting, held on October 19, 2018, they were briefed by the authors of these papers. They were also briefed by government officials—subject matter experts on governmental activities in the areas of technical standards, cybersecurity and privacy, and digital trade. Armed with this knowledge, the executives engaged in a facilitated discussion centered on two key questions for each of these three topics: (1) Which public policy issues/questions related to this topic are most important to advance smart manufacturing? (2) Apart from public policy issues, which specific steps or actions related to this topic would best advance smart manufacturing?

The remainder of this paper describes the perspective of these executives, gleaned from the facilitated discussion. To ensure an honest and rigorous dialogue, we promised to refrain from attributing particular comments to particular individuals or companies.

Technical Standards

As the Low paper acknowledges, there are hundreds of standards developed or under development that relate to smart manufacturing. Some groups are developing overarching "reference architecture" to conceptualize the

needed standards and help direct the efforts of Standards Development Organizations (SDOs) and others from around the world. But from the perspective of the firm, these efforts present a complicated labyrinth for navigation. As one participant pointed out during the meeting, "We have a series of stovepipes or silos, each with their own standards. How can we best integrate these?"

One common thread to the ensuing conversation related to the role of the U.S. government. The executives acknowledged that the governments of other countries, such as China and Germany, are more engaged in smart manufacturing standards than is the U.S. government, and that these nations are approaching it from a "top-down" perspective, where government convenes the process and directs the action, as opposed to the "bottom-up," market-driven approach that is more typical of how the U.S. government approaches the development of standards, where companies set the priorities for and lead in the development of high priority standards.

The participants did not see the U.S. approach as being clearly superior to that of Germany or China. And the U.S. has some advantages. As one participant noted, "The U.S. situation is not dire. For example, we have great technological expertise." And this expertise provides the U.S. with an advantage in the standard setting process.

One executive noted an advantage to the German approach, "Industrie 4.0 has provided certainty for investors. The U.S. government is not providing such certainty." There was a sense that smart manufacturing investment by manufacturers would be enhanced should clear global standards emerge.

Offered another participant, "The U.S. government should pursue portability of standards by getting other countries to accept/adopt [those developed here.]"

Although no one suggested that the U.S. government should prioritize its standard-setting efforts by adopting a top-down approach like that of China or Germany, there was sympathy/support for a more aggressive U.S. posture.

Offered one executive, "Germany and China have a strategic intent to garner competitive advantage. How can the U.S. leverage its strengths (e.g., technological expertise, high quality manufacturing processes and goods, etc.) to obtain a competitive advantage?"

Two participants suggested that manufacturers should join forces and ask NIST to focus U.S. government attention on a specific set of priorities for smart manufacturing standards. As one noted, if industry takes such action, NIST will respond as it has done so in the past with respect to other technologies. Another participant, building off this idea, suggested that industry focus on "somewhat settled" matters, where consensus is most easily attained. Such a cooperative approach could provide a competitive advantage for all of industry, a phenomenon described as "co-opetition." A successful example of co-opetition from the past would be the U.S. approach to the Y2K issue.

A second emerging theme from the discussion was a need to promote not only standards development, but also standards adoption, especially by small and medium enterprises (SMEs).

Said one executive, "There is not enough SME representation in standards development. Our large original equipment manufacturers (OEMs) drive standards." Said another, who works predominantly with small manufacturers, "SMEs need incentives to drive engagement—participating in development and also in adoption of standards." One participant offered a specific incentive—could the current R&D tax credit be used for standards development process? Although the question was not answered, it underscored a sense from the group that incentives are needed to bring small and medium manufacturers to the standards development table.

Cybersecurity and Privacy

Three themes emerged from the conversation on cybersecurity. The first theme is cybersecurity policy for manufacturing must be informed by the distinction between IT and OT. Requirements appropriate for IT are often inappropriate for OT.

Explained one executive, "The priorities for IT and OT are very different. In IT, the priorities are confidentiality, integrity, and availability (i.e., reliability), in that specific order. In OT, the ordered priorities are reversed: availability, integrity, and confidentiality." Recommendations or requirements for cybersecurity are written for IT may make little sense for OT. Said another executive, "OT requires a different approach to cybersecurity than IT."

After learning that proposed legislation in Congress would require patches to limit cyberattacks, another participant pointed out that "patches" are commonly employed in the IT world to limit cyber threats, but this technique would be unacceptable for OT in a manufacturing setting given the priorities of control and availability. In IT, a company can install a patch every week. In OT, a company may want to install a patch every decade—maybe. There must be no slowdowns, no disruptions to the manufacturing process. Other executives acknowledged that the proposed legislation is more suited to B2C than B2B.

A second theme emerging from the conversation was that smaller companies often lag behind larger companies in terms of awareness and adoption of cybersecurity measures, and this hurts all companies in the value chain. Said one executive, "I am a big fan of the NIST framework. But small companies are willing to take on more risk than their larger customers. SMEs are thus making risk decisions for us."

The requirements in the NIST framework, imposed by DoD on its supply chain, proved to be a challenge for smaller businesses. The fact that DoD backed off on enforcement allowed manufacturers to avoid the need to achieve fast and full adoption. One participant noted that without enforcement, people won't comply. Clarity on the rules is needed. Offered another, "Manufacturers are slow to change. We have a rusty and lazy asset syndrome. We need a drop-dead date for compliance." Said a third, "Some companies have separated their shop floor from the rest of the company to comply with NIST 1-800-71. This is bad for smart manufacturing."

One executive opined that U.S. manufacturers are adopting cyber protections more slowly than manufacturers in other countries, perhaps because U.S. supply chains are more diverse due to heavy outsourcing over the last 20 years. It would be a useful area of research to determine if other countries adopting smart manufacturing faster than the USA and, if so, to determine the reasons.

A third theme related to compliance. For example, some noted the difficulty in finding a single solution to ensure cybersecurity and compliance with regulatory requirements in the U.S. and around the world. Lamented one executive, responsible for global cybersecurity, "There is no single product I can buy to get cyber security to where it needs to be." Offered another, "There will always be multiple products to buy. The trick is knowing which few will get you 80% there."

Several observed the difficulty in tracking regulatory requirements for cybersecurity, as requirements are ever-evolving. In response, another participant identified a couple of online resources: the Global Cybersecurity Index and the Carnegie Endowment Cybersecurity Norms. Others observed that companies are loathe to report cyberattacks, yet such information is necessary as a warning system for others. In response, one participant noted that in recent years, private sector companies in the same line of business have created Information Sharing and Analysis Centers (ISACs), which work well in alerting all within a particular industry to emerging cybersecurity threats.

With respect to privacy, discussion centered on emerging national standards. As one executive said, "Companies want certainty over requirements to protect personal privacy and prefer a global standard over multiple national standards." When suggesting that a company should just adopt the EU General Data Protection Regulation (GDPR) as a global standard, others argued against it because while GDPR is strong in certain aspects, it is weak in others. And because the U.S. is likely to impose its own standard eventually (e.g., the NIST privacy framework under development) different from GDPR, a long-term reliance on GDPR makes little sense.

Several of the executives agreed that a risk management approach to privacy (underway at NIST) is the right approach given differences across companies in the manufacturing sector.

Digital Trade

Digital trade issues arise when the flow of information relating to smart manufacturing crosses national borders or when policies otherwise impact the flow of information within a nation. For example, consider a heavy piece of equipment, made in the U.S., that is able to transmit digital information about its activity. If a foreign country restricts the digital information that can be transmitted by this equipment, it will lessen the value of the product while benefitting a competitor product that does not have any digital capability. For manufacturers of "smart" products, the evolution of digital trade rules will have a big impact on their investment.

The executives raised more questions than answers about digital trade policy. There was agreement that digital trade policy will have a big impact on manufacturers, but it is not clear how the international rules will evolve, as pointed out in the Aaronson paper. While the U.S. policy is to support a free flow of information across borders, GDPR represents a different approach, while other countries (e.g., China) are restricting the flow of information much more (e.g., data localization requirements). Trade disputes have and will continue to arise and be decided before digital trade policy evolves enough to give manufacturers greater certainty.

Furthermore, the impact of a more certain digital trade policy options are likely to differ across manufacturing firms given the wide variety of circumstances firms face such as the countries in which they operate, their product offerings, and their business model.

One executive asked about data gathered by B2B firms—will the data be considered "personal" or "public" or something else (e.g., confidential business information) covered by trade agreements or local regulation? The question is unknowable today and will only become clearer over time, as trade policy evolves. Another participant said that emerging digital capabilities of medical devices raise critical questions about the data: Who owns it? Who controls it? Such questions should, ideally, be answered before the norms for digital trade policy are established.

Artificial Intelligence

Given the rapid expansion of AI-enabled applications in manufacturing, outlined in the Crandall paper, and the potential for realizing the promise of smart manufacturing, participants of the roundtable engaged in a discussion of its strengths and weaknesses.

The executives readily acknowledged the emerging importance of AI and the difficulty many are having attracting AI expertise into the manufacturing sector. New college graduates with AI expertise, said one participant, are attracted to the tech sector and companies like Google and Amazon and not attracted to enter manufacturing. The common lament was that AI talent is a scarce resource that greatly limits investment in smart manufacturing.

A few of the executives felt that current interest (hype?) in AI is a misplaced. To them, if a company identifies a problem, then maybe AI is an appropriate tool to address it. But acquiring AI expertise and then looking for a

problem to solve isn't productive. To these executives, the appropriate question is not "How can I utilize this cool new technology?" but rather "Can I monetize AI expertise in my business? If so, how?" To these executives, it is not enough to recruit someone with AI expertise, the person must also know enough about the particular business and the manufacturing process to be able to apply it. This makes recruitment even more difficult.

Part of the problem, noted one executive, is cultural; parents do not want their children to pursue a career in manufacturing. Several of the executives acknowledged a need to make manufacturing "cool" to young adults, especially those who do not believe manufacturing is high-tech.

A few of the executives inquired about the ability to audit and understand the rationale for a conclusion reached via machine learning. Upon hearing that AI-enabled conclusions are often impossible or prohibitively costly to understand via audit, the participants in the room turned the discussion toward practical applications.

A few of the executives acknowledged employing AI in their operations. Others acknowledged planning for it in the future. The Crandall paper, which distinguished between situations where AI performs well and situations where it does not, fostered some reflection on the experience of the executives in attendance.

According to one participant, "We use machine learning in specific applications where it can outperform a person. We reject it when it is predictive unless it provides actionable insight. If we cannot understand a result, we do not adopt it."

Another participant noted that his company uses AI to help identify and then code into a computer why a machine fails. This has replaced a labor-intensive exercise that, too often, was done haphazardly. In this particular application, employing AI improved the accuracy of the coding. And humans still check the AI-coded reason before it is accepted.

A third executive distinguished between AI as a decision-making tool ("it can help humans make decisions") and AI as a predictive tool. The company is utilizing AI to assist in decision making but sees predictive applications in the future.

The emerging consensus among the executives was that AI can be useful in some cases, especially if there's a human overseer. However, the consequences of a failure in a continuous manufacturing process are so severe that executives have a high degree of trepidation of AI and machine learning as a decision maker absent human oversight. As one executive noted, "Actionable insight is what we need from AI."

Conclusions

Today, vendors are pitching a myriad of "smart manufacturing" technologies and solutions to a very conservative sector of the economy. To many of the executives at the roundtable, investment in smart manufacturing is akin to placing a huge bet on an uncertain future, which will be shaped by rapidly changing technologies and slowly evolving rules.

Nevertheless, these executives believe that a smart manufacturing evolution is underway and represents a significant transformation of the production process.

Information governance issues associated with smart factories will require collective action to create an environment conducive to investment. Much of this collective action will or could be initiated by manufacturers themselves, working in coordination with government.

To advance information governance, government officials ought to know that manufacturers have certain unique characteristics relevant to policy. These characteristics include distinct priorities associated with IT versus OT,

the complexity of 21st century value chains, and the limited capabilities of smaller firms. Information governance for smart manufacturing must be informed by such considerations or it will fall short of its goals.

In some important policy areas such as digital trade policy and privacy policy, proactive steps that manufacturers can take are difficult to identify and recommend. Eventually, a more certain policy environment will emerge, which will allow for more informed smart manufacturing investment decisions.

Peer Reviewers: Stephen Gold, President and CEO, Manufacturers Alliance for Productivity and Innovation; Ward Melhuish, Partner, Grant Thornton; and Timothy Mealey, Cofounder and Senior Partner, Meridian Institute.

Appendix A

List of Participants in the Smart Manufacturing Roundtable

On October 19, 2018 in Washington, DC, Indiana University (IU) hosted a roundtable event on smart manufacturing. The meeting was organized by the IU Manufacturing Policy Initiative in collaboration with the Manufacturers Alliance for Productivity and Innovation (MAPI). Here is a list of participants and affiliations:

Susan Ariel Aaronson, Research Professor of International Affairs, Elliott School of International Affairs, George Washington University
Jack Adoline, Director of R&D/Innovation for Engineered Components, business unit for Barnes Group Inc.
Sudhi Bangalore, Global Vice President for Industry 4.0 at Stanley Black & Decker
Steve Barr, Vice President of Crane Business System (CBS) at Crane Co.
Ernest Begin, Executive Director of Information Security & Governance at Kaman Corporation
Keith B. Belton, Director, Manufacturing Policy Initiative, Indiana University
David J. Crandall, Associate Professor, School of Informatics, Computer Science, and Engineering, Indiana University
Mark Cybulski, Vice President, Information Technology at BorgWarner Transmission Systems (TS)
Brian Cyphert, CISO & Executive Director Global IT Infrastructure at MSA Safety
Andrew Flavin, Policy Advisor, International Trade Administration
Annika Freudenberger, Project Assistant, Meridian Institute
Kimberly M. Getgen, Vice President, Sales & Marketing at EnPro Industries, Inc.
Shawn Horner, Vice President of Corporate Strategy and Digital Initiatives at Parker Hannifin
Ajit Jillavenkatesa, Digital Economy Advisor, National Institute of Standards and Technology
John Kreul, Chief Information Officer and Vice President of Commercial Services & Quality at Bemis Company
Naomi Lefkovitz, Senior Privacy Policy Advisor, National Institute of Standards and Technology
Angus Low, Global Product Standards and Regulation Manager, Rockwell Automation
Frank Mangano, Executive Director of Infrastructure Services for ITT, Inc.
Wilfred Mascarenhas, Advisor for Data and Analytics in Manufacturing and Quality IT at Eli Lilly and Company
Darrell Massie, founder and Chief Technology Officer of Intelligent Power and Energy Research Corporation (IPERC)
William (Tom) Matthews, Senior Vice President, Technology and R&D at Lincoln Electric Company
Timothy Mealey, Senior Partner and Managing Director, Meridian Institute
Rick Morse, Vice President of Innovation and Digital Solutions at Rexnord
Ryan Olson, graduate student, School of Public and Environmental Affairs, Indiana University
Chris Peters, Chief Executive Officer of The Lucrum Group
Benn Reynolds, Chief Information Officer at Moog Inc.
Scott J. Shackelford, Associate Professor, Kelly School of Business, Indiana University
Keith Staninger, Portfolio Leader, Digital Solutions and Controls in the Compression Technologies and Services, General Industry Division of Ingersoll Rand
Pat Sweeney, Senior International Trade Specialist, International Trade Administration
Dhrupad Trivedi, Global CTO at Belden and President of Tripwire

Appendix B

Steering Committee

Keith B. Belton, Director, Manufacturing Policy Initiative, IU School of Public and Environmental Affairs
Tom Duesterberg, Senior Fellow for Manufacturing, Hudson Institute
Stephen V. Gold, President and CEO, MAPI
Susan Johnson, Senior Director of Development, IU School of Public and Environmental Affairs
Timothy Mealey, Co-Founder and Senior Partner, Meridian Institute
Ward Melhuish, Principal, Public Sector Practice, Grant Thornton LLP
Patrick Mulloy, Trade Attorney and Consultant, formerly served on U.S.-China Economic and Security Commission
Terry Straub, Co-Founder, Manufacturing Policy Initiative, Former Senior Vice President, U.S. Steel
Bradford Ward, Partner and Trade Attorney, International Law, King & Spalding