Automation Alley®

**This white paper originally appeared in Automation Alley's 2020 Technology in Industry Report**

# How Industry 4.0 Transforms Data Regulation & Protection

**Written by:**

**Christopher Heiden, MSA, MSIS**
*Associate Professor, Data Science*
Walsh College

**Marrci Conner**
*Instructor-Cybersecurity Program Lead*
Henry Ford College

**Robert James**
*Associate Dean*
School of Business, Entrepreneurship and Professional Development
Henry Ford College

Industry 4.0 and the advent of the Industrial Internet of Things (IIoT)—the use of smart sensors and actuators to enhance manufacturing and industrial processes—has created massive amounts of data never before envisioned; providing manufactures with real-time analytics that change the way companies operate around the globe.

Data analysis allows manufactures to predict machine failure and downtime, optimize their supply chain, detect product deficiencies, boost quality and efficiency, lower costs and gain valuable insights into customer behavior. However, these Big Data benefits also pose massive challenges for manufacturers as they face critical issues surrounding security, privacy and regulations.

There is no single principal data regulation or protection legislation in the United States (U.S.). Data regulation and protection in the manufacturing sector is controlled at the state and international levels, for product and technical compliance, safety, health and environmental protection. Data management in the manufacturing industry is further complicated by data sharing practices (between suppliers, manufacturers and customers), privacy laws, liability and intellectual property (IP) protection. These complex issues are difficult to resolve and are associated with measures that are also hard to enforce. Thus, there's a strong need for versatile and well-integrated controls for platform-wide data regulation, governance and policy enforcement within the manufacturing sector (Ismail A. T., 2019).

Data protection in manufacturing is necessary to protect and safeguard the data from external players. Keeping data of immense value safe while sharing it widely, often across international borders, is no easy task (Ismail N., 2018). Data protection is complicated further by a set of processes that must meet organizational and compliance issues, for example the General Data Protection Regulation (GDPR) set in place by the European Union in 2018, covering the personal data of any EU resident. Any company that has employees, suppliers or customers in Europe must comply with the regulation.

Are today's manufacturing leaders in compliance with global data privacy regulations? Are they properly protecting their data and that of their customers from cyber threats? This paper will examine how Industry 4.0 transforms data regulation and protection in the manufacturing sector; how these smart technologies will impact people, processes and technology now and in the future; and steps manufacturers can take to ensure they are leveraging their data in a safe and compliant manner.

# People

## *Now*

The implications of data gathering, data protection and cybersecurity are immense for the manufacturing workforce as new Industry 4.0 technologies introduces new standards, regulations and protocols. Currently, the U.S. does not have a formal national strategy regarding smart manufacturing standards other than to facilitate innovation and allow the best solution to emerge. There are active initiatives from multiple groups and organizations, including government organizations, such as the National Institute of Standards and Technology (NIST); organizations focused on standards development, such as Underwriters Laboratories; research institutes, such as Digital Manufacturing and Design Innovation Institute (DMDII) and Clean Energy Smart Manufacturing Innovation Institute (CESMII) within Manufacturing USA; and individual companies. As a general rule, the U.S. encourages a voluntary, consensus-based approach where government agencies participate when invited by industry.

Businesses have grown familiar with the probable business impact of having IT systems go down because of cybercrime or malware infection. However, the convergence of IT with operational technology (OT) introduces new significant risk factors and real-world threats, potentially

immobilizing a production line. We are now experiencing more connected environments coupled with unsecure IIoT environments, meaning more security risks, software vulnerabilities, data breaches, ransomware or even sabotage.

## *Future*

In the future, smart manufacturing will rely on highly integrated value chains, a collection and management of personal information (on workers, customers, and suppliers), which is increasingly subject to local, state, federal and international regulation, global digital trade and application of artificial intelligence (AI). With such a complex system, many risks and security vulnerabilities associated with the IIoT stem from a lack of basic security measures not being in place. Interoperability, exposed ports, inadequate authentication practices and obsolete applications are just a few of the many risks. Combine this with having inexperienced information technology (IT) professionals and a network directly connected to the internet and more potential risks are introduced into the manufacturing environment.

To counter some of the risks, manufacturing companies will need to look for people with strong collaboration and communication skills, who are comfortable working with new tools or processes. This will help new hires and existing employees develop their smart manufacturing skill set, especially if the business takes a cross-training or upskilling approach rather than replacing them (Kontzer, 2019). Some experts feel the most important thing to do is invest in capability building and cultural change. Upskilling in areas of analytics and digital technologies will prepare the workforce for the changing environment, make them ready for future learning and also keep them relevant (Wave, 2019). Another method for training smart factory employees is to gather employee buy-in. "Warehouse managers and employees may feel resistant to implement these changes within their IIoT systems in the beginning, especially with telematics. "With transparent education and training, it should be evident that these systems allow employees to be better at their job and even make their job easier" (Vavra, 2019).

# Processes

*Now*

As we move further into the current industrial age, almost every manufacturing process will change. Government regulation drives process in many industries, especially in manufacturing. Indicators of a mature regulatory process in all areas of manufacturing are not evident as subsequent regulations tend to "shift and replace" versus strengthen. As regulators shift into new positions, new technology and current restrictions may become inadequate. Of course, the description of "inadequate" shifts as much as regulations change. Society's regulatory structure is working to keep pace with the change in technology. What was considered safe yesterday is now questionable. As technology changes, the need for regulations comes about when reported problems occur; to the point where public outcry gains the view of the regulating bodies.

Attacks on an information system will always happen, thus, cybersecurity best practices must be an integral part of a company's cybersecurity defense plan. In the manufacturing process, attacks can take aim at a single system, or an entire infrastructure. The ultimate prize is the compromise of the system or infrastructure. When the system is a manufacturing environment, robot, or environmental system, the compromise can be detrimental for the workers, bystanders and infrastructure. For that reason, security must be at the forefront of any development process and use case testing.

While every manufacturer is different, following best practice process guidelines can help organizations deal with evolving data regulations. These include establishing a dedicated process for collecting information on existing and anticipated laws and regulations; performing ongoing risk management; building a security framework accredited by outside firms focused on data security, cybersecurity and privacy; and working with customers to ensure compliance is top of mind. (Janssens, 2018)

## *Future*

What will it take to maintain America's status as a leader in smart manufacturing while transforming data regulations and protecting data? To start, the U.S. needs a formal national data regulation entity (agency, taskforce, committee, etc.) This data regulation entity must have the authority to legislate formal national data regulation strategies for the U.S. Here are some additional recommendations from thought leaders in this area:

- Firstly, the National Research Council (NRC) should convene a committee to develop policy recommendations to advance smart manufacturing in the U.S. As part of its review, the council should take a hard look at the strategic actions of other nations, especially China and Germany.
- Secondly, Congress should reauthorize Manufacturing USA. The institutes created under this umbrella program to focus on smart manufacturing are working on the cutting edge of technology development and are almost certain to yield major advances. Aside from their technological roles, the institutes engage in important and pressing information governance issues, such as standardization.
- Thirdly, Congress should enact the proposed USMCA so that the United States can engage and shape the global landscape on information governance and digital trade.
- Fourthly, the Office of the United States Trade Representative (USTR), which oversees trade negotiations with other countries, should continue to bring cases to the World Trade Organization when other nations create rules for information governance that act as nontariff trade barriers (e.g., data localization requirements).
- Finally, NIST should continue developing a risk-based approach to privacy, which will represent an alternative to (and perhaps an improvement over) GDPR (Belton, 2019).

# Technology

## *Now*

Industry 4.0 manufacturers are not immune to challenges in the realm of changing technology, especially in the area of data protection. Today, there is a growing dependence on using cloud providers. The cloud provides an ability for Industry 4.0 manufacturers to store vital data and information remotely instead of an on-premise infrastructure.

Organizations are switching to the cloud to decrease costs along with allowing improved collaboration between stakeholders. Cloud services are forecasted to grow significantly. "Gartner forecasts that the cloud services market will grow 17.3% in 2019 ($206.2 billion USD) and by 2022, 90% of organizations will be using cloud services" (Durcevic, 2019). This forecast illustrates a dramatic shift from the usage of on-premise data technology to cloud-based services. The challenges to organizations that will adopt cloud computing technologies is: security, managing cloud spend, lack of resources, governance/control, compliance, managing multiple clouds, performance and building a private cloud (Durcevic, 2019).

## *Future*

As the digital transformation continues, our data is now shared and used by more platforms than ever—in the cloud and IoT devices, for example—and this trend will only increase. But this huge benefit comes with a cost. The more connected we become, the more vulnerable our data is (Dor, 2020). The World Economic Forum predicts that in 2020 and beyond businesses will begin to rethink their approach to data regulation and protection.

AI, for example, will dramatically accelerate the identification of new threats and responses to them, helping manufacturers to block attacks before they can spread widely. However, cybercriminals are also starting to take advantage of the same AI techniques to help them probe networks, find vulnerabilities and develop more evasive malware. In addition, future security solutions will need to evolve to new, flexible, cloud-based architectures that deliver scalable protection at speed. (Dor, 2020).

AI "can be used to disguise attacks so effectively that one might never know that their network or device has been affected" (Ramachandran, 2019). AI provides both an opportunity and a threat in data protection. Organizations can use this as an opportunity to use machine learning for cyber threat detection. The idea is to not rely on past data only, but to work on how to predict threats.

Organizations must use a systematic approach to employing technology in data protection. The organizations that use AI should have a process set in place. This systematic approach includes using tools that are leading the way. Natural language processing (NLP) is one such tool used by the AI systems to parse and collect information on cyberthreats (Laurence, 2019). NLP can be used to parse through blogs, articles and news postings to gather a list of current threats. NLP is an additional set of tools that the cybersecurity firm can employ in the development of cybersecurity threat detection and protection. Another example of a tool being utilized is machine learning technology, allowing software to recognize patterns in web requests and automatically block those that could be a threat (Bocetta, 2019). Traditional cybersecurity detection tools must adapt to new technologies. The utilization of AI and machine learning can only increase data protection by cybersecurity organizations.


# Action Items

- Technology is outpacing the knowledge and skills of our current manufacturing environment. The tools used within the cybersecurity field are constantly changing. Manufacturers must upskill their current workforce to prepare for long term adaptation of a smart manufacturing environment.
- Regulatory requirements lengthen the overall product development lifecycle and increase manufacturing costs. However, regulatory requirements are paramount to ensure a secure environment. Once developed and tested, tools should be deployed using cloud services. The adaptation of cloud services by Industry 4.0 manufacturers is creating a need for creation of new tools and emerging technologies to address new threats. The usage of AI technologies by cybersecurity organizations can help in threat detection. Thus, an organization can use AI to predictively detect possible attacks or threats.
- Currently, there is no single principal data protection legislation in the United States. The United States should establish a formal national data regulation entity with the authority to legislate formal national data regulation strategies for the U.S.

# About Automation Alley

Automation Alley is the World Economic Forum's Advanced Manufacturing Hub (AMHUB) for North America and a nonprofit Industry 4.0 knowledge center with a global outlook and a regional focus. We facilitate public-private partnerships by connecting industry, education and government to fuel Michigan's economy and accelerate innovation. Our programs give businesses a competitive advantage by helping them along every step of their digital transformation journey. We obsess over disruptive technologies like AI, the Internet of Things and automation, and work hard to make these complex concepts easier for companies to understand and implement.

## *Download the Full Report*

Automation Alley members are able to download the 2020 Technology in Industry Report free of charge! Log into your member portal and find your copy under the resources tab.

**Not a member?** Join Automation Alley today and let us help you increase revenue, reduce costs and think strategically. Contact 800-427-5100 or info@automationalley.com to learn more.

## *Copyright*



## *Our Contact Info*

2675 Bellingham
Troy, MI 48083-2044

Phone: 248-457-3200
Toll Free: 800-427-5100
Fax: 248-457-3210

Email: info@automationalley.com

Website: automationalley.com