UNIVERSITY OF PENNSYLVANIA
JOURNAL OF LAW AND SOCIAL CHANGE
Volume 25, Number 2 **2021**

CRITICAL PROTECTION FOR THE NETWORK OF PERSONS

BY JANINE S. HILLER*, GERLINDE BERGER-WALLISER**, AND AARON F. BRANTLY***

Abstract. The world is facing a future of sensored surveillance, filled with pervasive ultra-small connected devices, added to relatively larger ones already present in appliances and everyday technology today. Sensors will be bound to people as well as the environment, and people will provide much of the data that will compose the fundamental building blocks of a decisional infrastructure. Threats emanating from incompetence, unethical conduct, criminals, and nation states will put national security at increased risk because of new levels of potential harm to individual citizens as well as potential damage to physical infrastructure. A future that includes intimate electronic connections with a person's body creates an imperative to secure a Network of Persons (NoP), rather than of things. Sensor driven collection of huge amounts of data from individuals can impact the fundamental meaning of citizenship, affect economic prosperity, and define personal identity, all in a world composed of dwindling nodes of mediation between humans and automated systems. Intimately connected technology is increasingly interweaving persons in ways that extend the importance and relevance of critical infrastructure protections to the person. The present disjointed and fragmented approaches of Europe and the United States exacerbate the problems and elevate the importance of reconsidering designations of critical infrastructure. A new designation of a Critical Network of Persons (CNoP) does not obviate or alleviate the risks associated with the technologies; rather, it begins to shift the burden of risk mitigation and protection away from those least capable, towards the state and its partners. This paper proposes critical infrastructure protection for life critical functions in the NoP and argues that because the person is the building block for this critical infrastructure protection, the government's duty is qualitatively different from its duty to protect other critical infrastructures. Establishing a CNoP reorients the scope and focus to that of the citizen, the person—the building block of the nation. Ensuring the security at the individual level is imperative for maintaining national security for all.

* Professor of Business Law, Richard Sorensen Professor in Finance, Pamplin College of Business, Virginia Tech.

** Associate Professor of Business Law, School of Business, University of Connecticut.

*** Assistant Professor of Political Science, Department of Political Science, Virginia Tech. The authors are grateful to Mariah Fleming for her editorial assistance.

A human is sometimes considered as a 'thing' in public discourse related to IoT [Internet of Things].

–NIST, Networks of 'Things'

Act in such a way that you treat humanity . . . never merely as a means to an end, but always at the same time as an end.

–Immanuel Kant

INTRODUCTION

In November, 2017, the Food and Drug Administration approved a pill with an embedded sensor for use in the human body for the first time.[1] Intended to track whether a patient is taking a prescribed medicinal course of treatment, the sensor moves through the body and communicates with a patch worn by a patient, then sends information to an application on the patient's cellphone which forwards that information to a pharmaceutical company or a medical facility.[2] Another example for a pioneering sensor technology, "smart dust" about the size of a dust particle, is indistinguishable from the surrounding environment. Smart dust is a tiny sensor designed to collect data from the environment, physical connections, and persons—all of which are trackable to identified places.[3] The future will likely be filled with pervasive ultra-small connected devices in addition to the relatively larger ones already present in appliances and everyday technology today. Sensors will be bound to people as well as the environment, and people will provide much of the data that will compose the fundamental building blocks of a decisional infrastructure. Threats emanating from incompetence, unethical conduct, criminals, and nation states will put national security at increased risk because of new levels of potential harm to individual citizens as well as potential damage to physical infrastructure.

One such threat occurred in 2016, when one of the most broadly felt denial of service cyberattacks in the United States shut down the Internet in areas of the country for three hours because it preyed on vulnerabilities found in small Internet of Things (IoT) devices such as light bulbs and kitchen appliances.[4] Extrapolated to a future that includes an intimate electronic connection with a person's body, this incident foreshadows a time when there will be an imperative to secure an infrastructure that is connected to persons rather than things. When a plethora of devices—from ever

---

1 Pam Belluck, *First Digital Pill Approved to Worries About Biomedical 'Big Brother,'* N.Y. TIMES (Nov. 13, 2017), https://www.nytimes.com/2017/11/13/health/digital-pill-fda.html?emc=eta1[https://perma.cc/3MJF-G3RT]; Jonah Comstock, *In-Depth: How Digital Sensors Could Change The Face of Pharma*, MOBILE HEALTH NEWS (Nov. 17, 2017), http://www.mobihealthnews.com/content/depth-how-digital-sensors-could-change-face-pharma [https://perma.cc/6MVM-YUQU].

2 Belluck, *supra* note 1.

3 *See* Courtney Goldsmith, *Microscopic 'Smart Dust' Sensors are Set to Revolutionise a Range of Sectors*, NEW ECONOMY (June 3, 2019), https://www.theneweconomy.com/technology/microscopic-smart-dust-sensors-are-set-to-revolutionise-a-range-of-sectors [https://perma.cc/XTT9-D2PM](describing what smart dust is); Rebecca Rubin, *Smart Dust: Just a Speck Goes a Long Way in the Erosion of Fundamental Privacy Rights*, 15 J. HIGH TECH. L. 329, 342–46 (2015).

4 *See* Sam Thielman & Elle Hunt, *Cyber Attack: Hackers 'Weaponised' Everyday Devices With Malware*, The Guardian (Oct. 22, 2016), https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault [https://perma.cc/M6QK-B3YH].

present sensors embedded in streets to nanoparticles coursing through individual bodies—collect and share minutely and continually updated personal data, then the infrastructure to be secured will encompass the individual. While the IoT[5] and cyber-physical systems have captured our regulatory attention, technology is accelerating so rapidly that soon individuals will have granular connections with systems of sensors so embedded in the environment that it is no longer sufficient to contemplate societal expectations in an IoT. Instead, legal and social institutions must conceive of what it means to regulate and secure a different environment: an infrastructure substantially connecting individuals to critical systems at a personal level. Sensor-driven infrastructure collecting a huge amount of data from individuals can impact the fundamental meaning of citizenship, affect economic prosperity, and define personal identity, all in a world composed of dwindling nodes of mediation between humans and automated systems.

When we think of infrastructure in this new way, the values and human rights of persons are integral parts of the infrastructure in need of protection. To make this argument, Part I first establishes a basis for the belief that future cyber systems will evolve around connected persons and will soon be a reality. This Part then uses the National Institute of Standards and Technology (NIST) systems model to describe and define the attributes of such a personally connective system, that we call a Network of Persons (NoP). Part II describes the threats to and vulnerabilities of the NoP, and conceptualizes protection for life critical functions in the NoP. It argues that these life critical functions must become the focus of national security protection in the interest of the individual and the nation. Part III discusses how to achieve appropriate protection of the NoP infrastructure within national security protection. To this effect, it describes and compares U.S. and EU regulatory approaches to critical infrastructure protection, and analyses how these contrasting approaches translate to life-critical functions in the NoP. Because the person is the building block for this critical infrastructure protection, it is argued that the government's duty is qualitatively different than its duty to protect other critical infrastructures.

I. DEFINING THE NETWORK OF PERSONS (NOP)

Much has been written about the IoT, the Internet of Everything, and Cyber-Physical systems.[6] While there are degrees of difference, in this context the concepts are generally equivalent.

---

5 Arkady Zaslavsky, *September 2013 Theme: Internet of Things and Ubiquitous Sensing*, IEEE COMPUT. SOC'Y, https://www.computer.org/publications/tech-news/computing-now/internet-of-things-and-ubiquitous-sensing) [https://perma.cc/Y5B8-N4AV] (last visited Nov. 1, 2020) ("[T]he Internet of Things (IoT) will comprise many billions of Internet-connected objects (ICOs) or "things" that can sense, communicate, compute, and potentially actuate, as well as have intelligence, multimodal interfaces, physical/virtual identities, and attributes.").

6 NIST uses the term Cyber-Physical Systems, which includes the Internet of Things and "[s]mart anything." *Cyber-Physical Systems*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/el/cyber-physical-systems [https://perma.cc/5VQU-SFJ5] (last visited Nov. 1, 2020). Within the legal literature, see these leading articles: Scott R. Peppet, *Regulation the Internet of Things: First Steps Toward Managing Discrimination*, *Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014); Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6 (2015); There are many recent articles about the Internet of Things. *See generally,* Jane Kirtley & Scott Memmel, *Too Smart For Its Own Good: Addressing the Privacy and Security of the Internet of Things*, 22 J. INTERNET L., Oct. 2018; Nicole Smith, *Protecting Consumers in the Age of the Internet of Things*, 93 ST. JOHN'S L. REV. 851 (2019); Lawrence J. Trautman et al., *Governance of the Internet of Things (IOT)*, 60 JURIMETRICS J. 315 (2020); Charlotte A. Tschider, *Regulation the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENV. L. REV. 87 (2018).

Each describes a world of connected devices, usually employing a type of sensor that is designed to collect, or sense, information, and transmit the data, often by means of an Internet connection.[7] Multiple types of sensors are in use today in everyday life. Apple iPhone technology, for example, uses sensors in the process of facial recognition that are crucial to the mapping of a person's face in order to unlock the phone.[8] Audio sensors, such as those used by Amazon's Alexa,[9] can be used not only to respond to instructions or questions, but also to identify a person by her unique speech patterns.[10] The types and uses of sensors are almost endless, embedded in things such as smart buildings and cars and from wearable health fitness appliances to patient monitoring devices and smart pharmaceuticals.[11] Sensors are simply everywhere, and the future proliferation of sensors will be able to monitor and collect data about the most personal aspects of an individual's life.

Beyond current ubiquitous sensor applications, the advent of future and near-future technology will soon be reality. Although technology will continue to develop in unpredicted ways, a few illustrative descriptions of methods for an intensively, personally connected environment set the stage for what is to come. The technologies described here are on the cusp of realization and are used in limited circumstances or proof-of-concept rollouts today.

A. Person Level Connectivity

Forthcoming technologies significantly advance methods of sensing a person's existence and identity. [12] "Hypersensing" describes a technological tsunami of sensors collecting information that is fed into systems of machine learning based across industries and places.[13] Hypersensing means that the

---

[7] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-75, INTERNET OF THINGS: STATUS AND IMPLICATIONS OF AN INCREASINGLY CONNECTED WORLD 7 (2017) (describing the three layers as hardware, where sensors are located, network, such as Wi-Fi, and software, which is needed to collect the data).

[8] *See* JV Chamary, *How Face ID Works On iPhone X*, FORBES (Sept. 16, 2017, 5:00 AM), https://www.forbes.com/sites/jvchamary/2017/09/16/how-face-id-works-apple-iphone-x/#64e4da52624d [https://perma.cc/5HSR-27JU]; Michael deAgonia, *Apple's Face ID [The iPhone X's Facial Recognition Tech] Explained*, COMPUTERWORLD (Nov. 1, 2017, 2:57 AM), https://www.computerworld.com/article/3235140/apple-ios/apples-face-id-the-iphone-xs-facial-recognition-tech-explained.html [https://perma.cc/3M4Z-QQN9].

[9] *See* Jefferson Graham, *Alexa Guard Can Now Listen for Alarms—Or, Perhaps, a Cheating Spouse?*, USA TODAY (May 14, 2019, 9:40 AM), https://www.usatoday.com/story/tech/talkingtech/2019/05/14/alexas-latest-skill-listening-alarms-and-snooping-home-life/1189230001 [https://perma.cc/T3ZP-GEKB].

[10] *See* Omesh Tickoo, *Making Sense of Sensors—Types and Levels of Recognition*, APRESS (May 5, 2017), https://www.apress.com/gp/blog/all-blog-posts/making-sense-of-sensors/12253808 [https://perma.cc/A6B9-H36G].

[11] *See* Janine S. Hiller, *Healthy Predictions? Questions for Data Analytics in Health Care*, 53 AM. BUS. L.J. 251, 275–76 (2016) (explaining that patient mobile connected devices feed into health care data); Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things*," 2017 U. ILL. L. REV. 415, 418 (2017) (stating that "nearly everything not currently connected to the Internet, from gym shorts to streetlights, soon will be.").

[12] *See* Martin Geddes, *Introducing Hypersense & Human Technology*, DEWAYNE-NET (Jan. 31, 2015), https://dewaynenet.wordpress.com/2015/02/01/introducing-hypersense-human-technology [https://perma.cc/E9C6-R4BK].P5QK-9BZR]. Mohd Javaid et al., *Sensors for Daily Life: A Review*, SENSORS INTERNATIONAL (July 19, 2021), https://doi.org/10.1016/j.sintl.2021.100121 [https://perma.cc/7EGW-UFAT].

[13] Martin Geddes, *The Future of Everything: Making Sense of the Sensor Revolution from a Telecoms Perspective*, IEEE INTERNET OF THINGS (July 12, 2016), https://iot.ieee.org/newsletter/july-2016/the-future-of-everything-making-sense-of-the-sensor-revolution-from-a-telecoms-perspective.html [https://perma.cc/WV4C-86LA].

sensors first gather data, which is then processed in a computing system that will very quickly provide near-immediate feedback to a human decision maker. The synergy driving the concept is the combination of continual data feeds with machine learning, which is expected to improve prediction of behavior or events in real-time.[14] For example, police departments use body cameras today, but tapes are usually viewed when the need to download and review an event occurs. But bodycams may soon be able to provide real-time feedback to on-duty officers by using sophisticated facial recognition software to identify individuals within the officer's vision—even in a crowd.[15] When the system matches a face with a suspect or missing person in a database it conveys this information to officers who can decide whether to stop a person walking down the street.[16]

Smart dust is another specific technological example of sensors, data, and automated decision making that can be embedded and closely connected with individuals. [17] The term "smart dust" was coined in the 1990s by a professor at the University of California, Berkeley, to describe a research project for the Defense Advanced Research Projects Agency that had the goal to create a micro-sized sensor that included communication functionality.[18] Thus, the concept of smart dust, a sensor literally the size of dust that includes computing capacity and even perhaps a camera has been on the radar of legal scholars for a number of years.[19] Smart dust might also be considered a subset of nanotechnology, which has long been envisioned as a potential answer for many applications. For example, health care monitoring by nanotechnology applications are envisioned to move throughout the body and communicate health information and status.[20] Potential uses for smart dust, or motes, as it is also called,[21] are all-encompassing, and could monitor "anything that can be measured nearly everywhere."[22]

While there were barriers to the commercialization of smart dust in the past, in recognition of its progress, in 2017 Gartner Research placed it on the radar of innovative technologies with

---

14 The promise of "[t]his 'hypersense' revolution is big enough that you can make a good case that 'cognitive' is the new 'mobile'," because "[t]he ability to make sense of the 'hypersense' world enables new forms of contextual computing and communications. The machines can increasingly initiate action in the world on behalf of people. This is a collective phenomenon akin to the arrival of the Web in the 1990s. We might call it the 'Decision Matrix.'" *Id.*

15 *See* Shibani Mahtani & Zusha Elinson, *Artificial Intelligence Could Soon Enhance Real-Time Police Surveillance*, WALL ST. J., (Apr. 4, 2018), https://www.wsj.com/articles/artificial-intelligence-could-soon-enhance-real-time-police-surveillance-1522761813 [https://perma.cc/Z7UP-N37P].

16 *Id.*

17 Because neutral dust would require operation and installation within the brain, it is beyond the scope of this article but deserves a mention. *See generally* Elise Ackerman, *How Smart Dust Could be Used to Monitor Human Thought*, FORBES (July 18, 2013, 1:12 AM), https://www.forbes.com/sites/eliseackerman/2013/07/19/how-smart-dust-could-be-used-to-monitor-human-thought/#4bc8f2a27ebf [https://perma.cc/2Y83-E8QV] (describing the potential uses of neural dust).

18 Rubin, *supra* note 3, at 342–43 (describing the history of smart dust development).

19 Smart dust research began in the 1990s at the Universirt of California Berkeley. *Id.* at 342. *See* A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning From Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1719 (2015); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1538 (2000); Rubin, *supra* note 3, at 351; Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2329 (2007).

20 *See* Janet Brewer & Ogan Gurel, *Nanomedicine: Issues of Privacy and Informed Consent*, 6 NANOTECHNOLOGY L. & BUS. 45, 46 (2009).

21 Bernard Marr, *Smart Dust is Coming. Are You Ready?*, FORBES (Sept. 16, 2018, 11:52 PM), https://www.forbes.com/sites/bernardmarr/2018/09/16/smart-dust-is-coming-are-you-ready/#169a4c2a5e41 [perma.cc/2ASE-A3N8].

22 *Id.*

mainstream adoption predicted in 10 years.[23] Others also name it as one of the next most disruptive technologies, predicting that "the advent of smart dust will see the distribution of billions or trillions of devices, each capable of transmitting specific feedback. . . ."[24] Smart dust has a good chance of being part of the not-too-distant future environment in which individuals are almost continually subjects of data collection, and sensors collecting the data can do so at an individually and virtually invisible level.

Another example to illustrate the very intimate connection of devices and persons is digital twins technology.[25] Called the "Digital Twin of the Person" when applied to people, it is a technology on the rise, as predicted by the 2020 Gartner Hype Cycle for Emerging Technologies.[26] Using dynamic data collection, a "digital twin" of a person—a simulated and constantly updated digital version of the actual person—is created virtually.[27] Creating a digital twin of an individual by collecting and combining

---

[23] *See* Press Release, Gartner, Gartner Identifies Three Megatrends That Will Drive Digital Business Into the Next Decade (Aug. 15, 2017); *see also* Ami Marketing, *What in the World is Smart Dust?*, AMI (Oct. 3, 2017), https://ami.com/en/tech-blog/what-in-the-world-is-smart-dust [https://perma.cc/J9ZG-VEGB]

(confirming the promises and potential application of smart dust); Devin Coldewey, *IBM Working on 'World's Smallest Computer' to Attach to Just About Everything*, TECHCRUNCH (Mar. 19, 2018, 4:15 PM), https://techcrunch.com/2018/03/19/ibm-working-on-worlds-smallest-computer-to-attach-to-just-about-everything [https://perma.cc/9E72-MHAT] (giving an example of one potential application of smart dust).

[24] Tim Fryer, *20 Technologies to Change the World*, E&T MAG. (Sept. 22, 2017), https://eandt.theiet.org/content/articles/2017/09/20-technologies-to-change-the-world [https://perma.cc/J3N4-Z7YN].

[25] "While the concept has been floated for years, it is only since the introduction of IoT—and all the sensors, networking, and Big Data that may be included—that the Digital Twin has become a financially viable concept to implement." Charlie Osborne, *Digital Twin Initiatives Set to Take Enterprise Center Stage: Gartner*, ZD NET (Mar. 13, 2018), http://www.zdnet.com/article/digital-twin-initiatives-set-to-take-center-stage-in-the-enterprise-gartner [https://perma.cc/RNW6-8LF9]*; see also* Daniel Newman, *Digital Twins: The Business Imperative You Might Not Know About*, FORBES (May 30, 2017, 11:28 AM), https://www.forbes.com/sites/danielnewman/2017/05/30/digital-twins-the-business-imperative-you-might-not-know-about/#12052a0693c3 [https://perma.cc/W49N-T43W] (explaining how digital twins can benefit collaborations within an enterprise).

[26] Kasey Panetta, 5 *Trends Drive the Gartner Hype Cycle for Emerging Technologies, 2020*, GARTNER (Mar. 8, 2021), https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020 [https://perma.cc/TV8X-A9EH].

[27] "Whenever [the] physical world changes, a physical sensor tries to update the current status to its digital twin representative in the cloud. Every physical thing and its corresponding cyber thing manages a Data Store. Every physical or cyber thing is identified by a unique ID (i.e. IPv6, Universal Product Code (UPC), Electronic Product Code (EPC), etc.) and is aware of the existence of its twin counterpart." Kazi Masudul Alam & Abdulmotaleb El Saddik, *C2PS: A Digital Twin Architecture Reference Model for the Cloud-Based Cyber-Physical Systems*, 5 IEEE ACCESS 2050, 2053 (2017). *See also* Christian Sarkar, "*Digital Twins, IoT, and the Future of Business" —An Interview with Sanjay Sarma,* THE MKTG. J. (Apr. 25, 2017), http://www.marketingjournal.org/digital-twins-iot-business-sanjay-sarma [https://perma.cc/N3KY-PU9Y] (explaining the potential effect digital twin can have on the business world). The reason for creating a digital twin of a *physical* object is usually to model future performance and apply predictive analytics to inform decisions about the object related to efficiency, maintenance, or replacement. Development is advanced for industrial systems. General Electric is well known for its digital twin product for industrial systems, with over 500,000 in use today; it describes them as a progression towards "symbioses between human minds and machines." Roberto Saracco, *The Rise of Digital Twins*, IEEE FUTURE DIRECTIONS (Jan. 16, 2018), http://sites.ieee.org/futuredirections/2018/01/16/the-rise-of-digital-twins [https://perma.cc/D9WQ-ARQR]; *see also* Osborne, *supra* note 25 ("Gartner revealed the results of a survey [] which suggests that 48 percent of companies which are already enjoying the benefits of IoT are using, or plan to use Digital Twin by the end of 2018."). The use of digital twins is also proposed for use in Smart Cities to manage and predict system functions. *See* Alam & El Saddik, *supra* note 27, at 2050 (explaining that "physical systems act as the sensors to collect real-world information and communicate them to the computation modules

very personal information can be used, for example, to predict illness and for medical treatment.[28] Retail industries are not far away from using digital twins to create a replica of each consumer, using both purchase and non-purchase data in order to make predictions about individual consumer behavior in order to "cross-sell and up-sell."[29]

In 2017, Deloitte explained that as applied to physical assets, "[t]he digital twin is based on massive, cumulative, real-time, real-world data measurements across an array of dimensions."[30] It is not hard to see that it would be a relatively small step for the data from wearables and smart dust to be fed into a multi-use digital twin of an individual.[31] Massive and real-time data collection about a person may be the foundation of Facebook's metamorphosis in 2021 into a company called Meta, which it premised on a future of an "embodied internet."[32]

Decisional uses of technology such as real-time police bodycam systems, smart dust, digital twins, and the like, fall into the broader category of cognitive computing, augmented reality, machine learning, or deep learning that can all be considered to fall under the general umbrella of artificial intelligence.[33] The illustrative technologies are exemplary of a pervasive environment of individually-based data collection and analysis. The data collected by sensors is transferred, usually through the Internet, to computing systems that can make sense of large datasets and can combine sensor data with additional datasets. Finally, automated systems will create predictions, shared at some level with

---

(i.e. cyber layer), which further analyze and notify the findings to the corresponding physical systems through a feedback loop.").

28 *See* Koen Bruynseels et al., *Digital Twins in Health Care: Ethical Implications of an Emerging Engineering Paradigm*, 9 FRONTIERS GENETICS 1, 3 (2018) (stating that "[t]he emerging data-driven personalized health care practices bear striking resemblances to Digital Twins driven engineering in industry."). *See generally* Min Chen et al., *Smart Clothing: Connecting Human with Clouds and Big Data for Sustainable Health Monitoring*, 21 MOBILE NETWORKS & APPLICATIONS 825 (2016) (describing how data collected through smart clothing and other technologies can allow people to better recognize health issues and resolve them more quickly).

29 Todd Hassell, *How 'Digital Twins' Nurture the Customer Experience*, FORBES (Jan. 11, 2018, 8:16 AM), https://www.forbes.com/sites/sap/2018/01/11/how-digital-twins-nurture-the-customer-experience/ [https://perma.cc/7NT4-MVF8].

30 Aaron Parrott & Lane Warshaw, *Industry 4.0 and the Digital Twin*, Deloitte (May 12, 2017), https://www.deloitte.com/us/en/insights/focus/industry-4-0/digital-twin-technology-smart-factory [https://perma.cc/S6LF-PQ66].

31 *See* Macy Bayern, *Let's Get Phygital: Most Disruptive Tech of 2020*, TECHREPUBLIC (Nov. 11, 2019, 12:00 PM), https://www.techrepublic.com/article/lets-get-phygital-data-automation-and-iot-lead-the-way-in-disruptive-tech [https://perma.cc/3YN3-KJNK] ("As internet of things (IoT) devices continue advancing, from sensors to wearables and smartphones, more data points about humans will be collected. Humans will generate enough data to create a digital twin. . . ."); *see also* Diane J. Cook & Narayanan Krishnan, *Mining the Home Environment*, 43 J. INTELL. INFO. SYS. 503 (2014) (describing types of smart home monitoring sensors, data mining algorithms and uses, and privacy and security challenges).

32 Kevin Kruse, *The Metaverse, Digital Twins, and Leadership Development*, FORBES (Nov. 4, 2021), https://www.forbes.com/sites/kevinkruse/2021/11/04/the-metaverse-digital-twins-and-leadership-development/?sh=63a8a9186287 [https://perma.cc/2DUV-LFNM] ("[B]efore there can be a true metaverse—enterprise or otherwise—there must first be 'digital twins'.").

33 NAT'L SCI. & TECH. COUNCIL, EXEC. OFF. OF THE PRESIDENT, PREPARING FOR THE FUTURE OF ARTIFICIAL INTELLIGENCE, 6–11 (2016) (stating that "There is no single definition of AI [Artificial Intelligence] that is universally accepted by practitioners." *Id.* at 6); *see also* Andy Meek, *Connecting Artificial Intelligence with the Internet of Things*, THE GUARDIAN (July 24, 2015, 7:11 AM), https://www.theguardian.com/technology/2015/jul/24/artificial-intelligence-internet-of-things [https://perma.cc/3F9N-AG5K].

decision makers, or instituted in an automated decision-making process, based on the data and analysis. The impact is that:

> [These] computing systems redefine the nature of the relationship between people and their increasingly pervasive digital environment. They may play the role of assistant or coach for the user, and they may act virtually autonomously in many problem-solving situations. The boundaries of the processes and domains these systems will affect are still elastic and emergent.[34]

In summary, the personally connective system is not science fiction. As technology becomes available to connect any number of identified, specific persons at a granular level, and as these form networks that allow for further communication, persons will be the target for threats and vulnerabilities in ways not previously imagined and at exponentially higher levels. Thus, the security of the personally connective system raise many legal, ethical, and social issues, discussed in the following parts.

The elements of the system described in general in Part I. A. include a hypersensed environment consisting of the sensored and connected person, large amounts of data collected to make predictions about individuals, and the technological means of closing the data loop with decision making. The following section describes an earlier effort by the National Institute of Standards and Technology (NIST) to create a systems approach to describe the interlocking parts and processes in a network as it applies to things. Part I. C. will extend the NIST model to include the personal sensoring described here.

B. The NIST Systems Model

In 2016, NIST issued a publication entitled 'Networks of 'Things.'"[35] The goal of the publication was to create a vocabulary for discussing the commonly referred to IoT, smart systems, or whatever name is used for a distributed system that communicates via the Internet or another medium that transmits data.[36] Acknowledging that "[no] simple, actionable, and universally-accepted definition for IoT exists," it nonetheless identified that "[t]he tethering factor [connecting converging technologies] is data."[37] The NIST vocabulary and descriptive model provides a common understanding of the basics of a sensored world, how it "behaves," and how such a system relates to the creation of trust.[38] Applying a simplified model, but building upon the NIST work, a definition of a Network of Things (NoT) can be described as consisting of five elements: 1) sensors, 2) aggregators, 3) a communication channel, 4) external or e-utilities, and 5) decision triggers.[39]

---

34 Sue Feldmen & Hadley Reynolds, *Cognitive computing: A definition and some thoughts*, KM WORLD, https://www.kmworld.com/Articles/News/News-Analysis/Cognitive-computing-A-definition-and-some-thoughts-99956.aspx. [https://perma.cc/XF5K-UBC6]

35 Jeffrey Voas, NETWORKS OF 'THINGS' 1 NAT'L INST. STANDARDS & TECH (2016) (NIST uses the acronyms IoT (Internet of Things) and NoT (Network of Things) interchangeably but notes that "IoT is an instantiation of a NoT," Network of "ThingsSTANDARDS & TECH., ").

36 *Id.* at 1 (as such the NIST definition of NoT includes but is not limited to the IoT).

37 *Id.*

38 *Id.* NIST decided that it is the behavior that matters, rather than an explicit definition.

39 *Id.* at 2.

According to NIST, the sensor elements of a NoT are: a sensor with a physical presence, it may be connected to the Internet, and its product is data.[40] Furthermore, sensors may or may not perform identification functions, the data that they transmit may or may not be accurate, and the data may be shared with any number of networks.[41] NIST identifies security as a potential concern for sensors, but suggests that security is only necessary under certain circumstances.[42] Particularly relevant to our discussion of security for a sensored network that evolves around persons, humans are described as possible threats to sensor reliability because they may fail to follow policy, misread data, or misplace sensors.[43]

While sensors produce the data, the aggregator component is defined as the software that processes that raw data, thus making "big data" usable.[44] Security and reliability of the aggregator software is a concern, as it may be hacked, blocked, or misled by incorrect data.[45] Next, the communication channel is the transportation layer, moving the data "from intermediate events at different snapshots in time."[46] The Internet, or wireless communication, is likely to be the communication channel. However, a mesh network could allow communications directly between sensors.[47] Communication channels can also be attacked or slowed, and their reliability and security are concerns. Next, an e-utility is defined as a "software or hardware product or service."[48] Other standard-setting bodies have named this part of the system as being comprised of "*cyber-entities*," or "*digital entities*."[49] These entities "execute processes or feed data into the overall workflow."[50] Interestingly, NIST classifies *a human* as a possible e-utility.[51] If an e-utility is not human, it may still have a unique ID. Although NIST did not explicitly recognize this fact, we argue that an e-utility that has a unique ID may be so closely connected to an individual that, in many ways related to data collection, it serves similar functions.[52] Both reliability and security continue to be issues for the e-utility.[53]

The final element of the NoT is the decision trigger(s). NIST describes this element as an "if-then" function that "define[s] the end-purpose" of the NoT and "can control actuators and transactions."[54] For example, a decision trigger might be part of a smart city infrastructure that monitors

---

40 NIST describes twenty-nine attributes of a sensor. *Id.* at 2–4.

41 *Id.*

42 *Id.* at 3-4.

43 *Id.* at 4.

44 *Id.*

45 *Id.* at 5.

46 *Id.* at 7.

47 *See* Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1005 (2016) (stating that "[i]n a mesh network, devices connect directly with one another to relay information, enabling the network to sprawl over a wide area even though a single device may transmit only up to 300 feet.").

48 Voas, *supra* note 34, at 9.

49 *Id.* at n.3.

50 *Id.* at 9.

51 *Id.* at 10.

52 *See infra* Part II.B.

53 *See* Voas, *supra* note 34, at 11-13.

54 *Id.* at 11-13. Andrea Matwyshyn analyzes a similar, but distinct, infrastructure that she names the "Internet of Bodies," that not only uses sensors but that is also uniquely embedded into human bodies. Andrea M. Matwyshyn, *The Internet of Bodies*, 61

air quality: sensors collect air quality data that is aggregated across a geographical area, and if software (the e-utility) determines that the air quality reaches an unacceptable point, then the decision trigger might be programmed to close city streets to further traffic.

The following chart summarizes each element of the NoT, and gives a basic example:

	NIST NoT	**Example**
Sensors	Collect data	Car maintenance data collected by onboard computer; apps in car; mobile phone apps
Aggregators	Process data from multiple sources and times	Car manufacturers or their business associates
Communication Channel	Network(s) that transfer data	Internet; proprietary network
External/E-Utilities	Products or services that use data for particular purpose	Navigation services; emergency crash response; roadside assistance
Decision Trigger	Action taken as result of data collection and processing: an if-then process.	Data from car indicates that both tire pressure is low and the car has missed its last service; location indicates a dealer is close by; message sent to driver with address of dealer

C. Modifying the NIST Model for the NoP

We propose an update to the NoT that identifies a person-level sensoring environment, naming this the Network of Persons (NoP). The NoP building blocks are interconnected *persons* based on 1) targeting of individuals, 2) collecting and processing data, and 3) triggering decisions about a person based on the data. Like the NIST NoT, this proposed definition recognizes that data fuels the system. Utilizing the five NIST elements but fine-tuning those definitions, we describe the NoP as consisting of personally targeted[55] sensors, aggregators that operationalize and combine data that is related to persons, e-utilities that process the data, and triggers of person level decisions. Importantly, an individual person must be affected by the NoP, but the point in the system at which the person is affected may vary. The next sections further describe the elements of the proposed NoP.

1. Targeting a Person's Data: Sensors and Aggregators

Similar to the NIST definition, sensors in the NoP may or may not collect personally identifying information. Our proposed definition of NoP sensors is that they must either be physically connected to a person, or be so closely aligned with a person that they are targeting the person's data. This definition varies from the NIST approach to a NoT, and it eliminates purely industrial and

WM. & MARY L. REV. 77 (2019).

55 *See infra* Part I.C. "Personally targeted" is based on the systematic use of external sensors to collect and process information about the person. This is different from, but can include, the traditionally defined personally identifiable information.

environmental sensors that collect information unrelated to an individual. It includes sensors that are physically or proximately connected to a person, such as health related monitors or physical activity monitors, and it encompasses a broader set of ubiquitous sensors, exemplified by future smart dust, that are not physically connected to a person but are nonetheless targeted towards sensing data related to persons.

NIST discussed the reality that a sensor may collect incorrect data and that it may share data more broadly; these realities are also faced by an NoP sensor—with potentially devastating consequences. In contrast to the NIST assumption that security is not always a necessity for sensors, it is proposed that security is, indeed, always needed for NoP sensors,[56] because they are focused on critical life functions.[57]

NoP aggregators perform similar functions to aggregators in the NIST model, operationalizing the person's data so that it is useful to an e-utility. The proposed model of an IoP includes the possibility that an aggregator's processing of nonpersonal data might be combined with additional data, resulting in the targeting of a specific person. An aggregator, in sum, can process non-attributed data into a form that will be part of a NoP.

NIST explains that security is a problem for aggregators, because they may be hacked or compromised, or they may process incorrect data.[58] These security concerns are amplified in an NoP, because the sensor data that targets a person, aggregated with other data, can create a new and elevated threat of harm at the personal level. Coding errors or manipulated data could also cause aggregators to produce flawed results that would create systematic failures.

2. Connective Tissue: Communication Channels

The various communication channels in the NIST model are the same for an NoP, as the data will need to be communicated so that it may be transformed, processed, and applied to make decisions. However, it is important to note an essential component of an NoP: that the location of the communication network (and the entire system) may one day happen in a physical place that is connected with, closely allied to, or even part of the person herself. For example, a pacemaker embedded in a person today is interrogated by means of a monitor, which then communicates information through an Internet connection to a medical data warehouse.[59] Based on this information, the pacemaker can be recalibrated.[60] However, in an NoP, a communication channel does not necessarily imply a physical distance. It is not difficult to imagine a time when technology will progress to the point that the entire process of sensing a patient's interaction with a pacemaker, interpreting the output, comparing the data to normal functions, and making a decision about the patient will be self-

---

56 We acknowledge that security requirements could differ based on different risk factors, as described in the NIST Cybersecurity Framework. *See generally Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. STANDARDS & TECH. (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [https://perma.cc/5VE5-6EME].

57 Which will be discussed in Part II.B.

58 Voas, *supra* note 34, at 5.

59 Katina Michael, *Implantable Medical Device Tells All: Uberveillance Gets to the Heart of the Matter*, 6 IEEE CONSUMER ELECS. MAG., Oct. 2017, at 107, 108.

60 *See id.* (describing data being retained and the device receiving firmware updates).

contained in a NoP that is embedded in and executed within the patient's body.[61] In situations such as those, and as multiple, personally targeted sensors communicate directly with each other, the communication channel is literally taking place at the level of the person herself. This example shows the critical importance of a secure NoP for both personal and national safety.

3. Individual Impact: NoP E-utilities and Decision Triggers

In comparison to the NoT, which can, for example, include real time operational inputs to a machine in a plant, our definition of the NoP e-utilities working with decision triggers processes large amounts of information in order to make decisions that affect *individuals*. For example, smart transportation is one part of an overall push to create sustainable smart cities that collect and use broad types of citizen data to make decisions about effectively managing services.[62] A 2014 white paper by the U.S. Department of Transportation described smart cities in this manner:

> [S]mart/connected cities contain and use "intelligent infrastructure," . . . devices and equipment that can sense the environment and/or their own status, send data, and often, receive commands. This intelligent infrastructure connects the city's world of data with its physical reality, creating data based on the real world and following data-based commands to act on the real world as well. . . . [S]mart/connected cities use new analytical processes that have been facilitated by ICT advances. These include big data analysis, crowdsourcing to gather data and solve problems, and gamification to incentivize behaviors and engage the connected citizen.[63]

This definition of a smart, connected city incorporates the fundamental elements of a NoT:[64] sensors to collect information and feed it into aggregators to process the raw data,[65] communication channels between multiple points of the network and the world, and e-utilities to process the data and use it to execute commands according to decision triggers.[66] Many interlocking systems will be required to achieve this vision, and it is not difficult to anticipate that a good deal of the data, although not all, will be targeted towards the individual as a driver or passenger, as the USDOT states: "[c]onnected vehicles and travelers will be able to share data with all sorts of equipment, *not only* transportation-related devices and infrastructure." [67] Sensors will certainly not always target data from persons, for

---

61 Mark Peyrot & Richard R. Rubin, *Patient-Reported Outcomes for an Integrated Real-Time Continuous Glucose Monitoring/Insulin Pump System*, 11 DIABETES TECH. & THERAPEUTICS 57, 57–61 (2009).

62 *See* Janine S. Hiller & Jordan M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, 68 HASTINGS L.J. 309, 323–34 (2017).

63 U.S. DEP'T TRANSP., THE SMART/CONNECTED CITY AND ITS IMPLICATIONS FOR CONNECTED TRANSPORTATION 1 (2014), https://www.its.dot.gov/itspac/Dec2014/Smart_Connected_City_FINAL_111314.pdf [https://perma.cc/3GNL-P3ED].

64 *See supra* Part I.B.

65 *See* U.S. DEP'T TRANSP., *supra* note 62, at 1.

66 *See generally* Tiffany Fishman & Justine Bornstein, *The Rise of Mobility as a Service,* DELOITTE INSIGHTS (Jan. 23, 2017), https://www2.deloitte.com/insights/us/en/deloitte-review/issue-20/smart-transportation-technology-mobility-as-a-service.html [https://perma.cc/7VZ2-YPKX] (providing a clear explanation, with example of the elements).

67 U.S. DEP'T TRANSP., *supra* note 62.

example they could be limited to only collecting data only about the number of cars on the road.[68] However, based on the USDOT vision to "target . . . *probable* safety violators"[69] and change driver behavior,[70] it is clear there would be infrastructure that targets data from individuals within such a system; linking mobile phones, smart car identifiers, and other connected devices to a person.[71] If used generally, and anonymously, an analytics service/product, for example one that manages traffic lights, would not be part of the NoP. On the other hand, a traffic e-utility might be designed to collect information for use in a predictive analytics application to track individuals in order to prevent crime; it would likely process personally-targeted data from transportation-related sensors to predict who is expected to commit crimes based on who they visit and the times and places they interact.[72] This use of an e-utility would be part of the NoP because it affects personal freedom of movement and rights of association that are critically important for citizenship and personhood. A decision trigger might, for example, be implemented in order to set insurance rates at a higher level if sensors detect that an individual frequents geographic areas that have high crime rates.

The following chart builds upon the previous NIST NoT description, and shows how each element is modified in the proposed NoP:

	NIST NoT	**Proposed NoP**
Sensors	Collect data	Data collection targets persons; physically connected or closely aligned with the person
Aggregators	Process data from multiple sources and times	Combines data in ways that continue, or create, targeting of persons
Communication Channel	Network to transfer data	Person is usually, but not always, an element of the communication channel
External/e-utilities	Products or services that use data for particular purposes	Product or service relates to an individual
Decision Trigger	Action taken as result of data collection and processing	Decision/action affects individuals

Having identified a Network of Persons, Part II outlines threats to and vulnerabilities of the system. In response to these threats, we propose that critical parts of the NoP deserve heightened

68 Fishman & Bornstein, *supra* note 65, at 121 (noting that Singapore's government shares information anonymously with private sector companies).

69 U.S. DEP'T TRANSP., *supra* note 62, at 2.

70 *Id.*

71 *See, e.g.*, *Internet of Things*, GSMA, https://www.gsma.com/iot/automotive [https://perma.cc/PN76-FQF3] (describing vehicles connecting with other vehicles, infrastructure, and people) (last visited Nov. 1, 2020).

72 *See* Exec. Off. of the President, Big Data: Seizing Opportunities, Preserving Values 1, 31 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/UL7G-56G7] ("Controversially, predictive analytics can now be applied to analyze a person's individual propensity to criminal activity," and therefore it "shift[s] the focus of predictive policing from geographical factors to identity.").

protection: when data is collected and/or aggregated through the sensors and, as a result, decisions are made that are applicable to "critical life" functions, the NoP is placed within the types of infrastructure that have been categorized as critical infrastructure.

II. ENVISIONING A CRITICAL NOP

In light of forthcoming technology on one hand, and growing technological disruption on the other, critical infrastructure protection is a priority, not only for the United States, but for security policy makers in developed economies around the world.[73] Assessing the nexus of critical infrastructure and identifying those areas where rights and national security concerns intertwine indicates areas where global standards or norms might be developed. By focusing on the subject, i.e. the person, at the center of the infrastructure the human importance is interwoven with the technical application. Below we establish the life-critical functions of the subject, the technical infrastructure upon which they depend, the vulnerabilities embedded in both, the relationship between the subject and the technology, and the logic for critical protection that the relationship necessitates.

A. Threats, Vulnerabilities, and National Security

It is increasingly difficult to disaggregate the human-digital relationship. As the relationship between persons and the digital world deepens, digital and human rights violations are likely to increase both in volume and severity. The result is that persons will be subject to threats, both materially and cognitively, for which they have no individual defense.[74] The imbalance between individual interactions within the digital ecosystem, and their ability to maintain their security in the face of criminal and state interference is well-documented. Report after report demonstrates that criminal entities, private enterprise, and state entities collaborate to undermine the fundamental privacy and security of devices used by individuals, threatening journalists, human rights activists, and the average citizen.[75] The

---

[73] *See also* Jing de Jong-Chen & Bobby O'Brien, *A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China*, WILSON CENTER, 11 (Nov. 2017), https://www.wilsoncenter.org/sites/default/files/media/documents/publication/approach_to_critical_infrastructure_protection.pdf [https://perma.cc/C98X-TBFK] (recommending global collaboration to protect critical infrastructure). *See generally Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, OECD (2012).

[74] Aaron Franklin Brantly, *The Cyber Losers*, 10 DEMOCRACY & SEC. 132, 142–43 (2014) (arguing that the development ever advanced cybersecurity technologies by nation-state actors substantially disadvantage individual citizens and consequently expose them to increasing levels of risk).

[75] *See generally, e.g.*, Jeffrey Knockel et al., *We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus*, CITIZEN LAB (May 7, 2020), https://citizenlab.ca/2020/05/we-chat-they-watch [https://perma.cc/5MEB-YBTJ]; Christopher Parsons et al., *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*, CITIZEN LAB (June 12, 2019), https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry [https://perma.cc/JJ7F-CNR7]; John Scott-Railton et al., *Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague*, CITIZEN LAB (Nov. 27, 2018), https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague [https://perma.cc/4RC5-ECFG]; Geoffrey Alexander et al., *Familiar Feeling: A Malware Campaign Targeting the Tibetan Diaspora Resurfaces*, CITIZEN LAB (Aug. 8, 2018), https://citizenlab.ca/2018/08/familiar-feeling-a-malware-campaign-targeting-the-tibetan-diaspora-resurfaces [https://perma.cc/PCA6-SPML].

proliferation and diversification of sensors in ways such as smart dust, digital twins, and future technologies portend a groundbreaking shift in the separation of the individual from the collective; the digital from the non-digital. Even today, it is nearly impossible for the citizenry of most developed, and many developing, nations to live their daily lives without generating data exhaust that is commoditized and used to shape behaviors.[76]

The diverse landscape of vulnerabilities and threats to individuals within cyberspace, both as autonomous agents and participants in larger networked environments, makes clear the national security implications resident within the NoP. One way to address these concerns is through critical infrastructure protection. In the aftermath of the 9/11 terrorist attacks, the USA Patriot Act created a statutory basis for critical infrastructure protection,[77] defined as "sectors that compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[78] The conditions that make critical infrastructures particularly susceptible to disruption include: a broad range of potential attacks, interconnectivity of sectors, high density of targets, and inadequate security[79] are also present in the NoP. Different levels of data collection, processing, and decision triggers in the NoP provide various points for attack. E-utilities are a means to join interconnected systems, and aggregators by their nature increase the density of data to be targeted and consequently enhance the rewards associated with successful attacks. Personally connective IoT devices continue to proliferate without adequate security and are likely to do so for the foreseeable future. A 2018 General Accounting Office (GAO) report indicates that cyber attacks could be weaponized, and it identifies attacks on personal health information as an example, stating: "Adversaries could also launch cyber attacks on the U.S. health care system, threatening patient safety by disrupting access to medical care."[80] The identification of this threat is more chilling when combined with the facts that aggregate health care data is increasingly collected through patient sensors and combined with ubiquitous lifestyle information,[81] and that 2018 was a record year for administrative enforcement actions due to health data breaches.[82] The disruption of citizen health is certainly a national security problem, as the COVID-19 pandemic so recently brings to bear.[83]

---

76 SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 130–38 (2019) (engaging in a process of behavioral surplus accumulation. This accumulation shifts individuals from economies of scale to economies of action, in which consumer behaviors are shaped).

77 Even before the 9/11 attacks, Presidential Directives addressed protection of critical infrastructure following terrorist attacks. *See* Joe D. Whitley et al., *Homeland Security, Law, and Policy Through the Lens of Critical Infrastructure and Key Asset Protection*, 47 JURIMETRICS 259, 261–63 (2007) (reviewing a series of Presidential directives and Homeland Security directives between 1996 and 2003).

78 *Id.* at 260.

79 Whitley, et al. identifies these conditions as key vulnerabilities. *See* ZUBOFF, *supra* note 75, at 268–71.

80 U.S GOV'T ACCOUNTABILITY OFF., REPORT TO CONGRESSIONAL COMMITTEES: NATIONAL SECURITY: LONG-RANGE THREATS FACING THE UNITED STATES AS IDENTIFIED BY FEDERAL AGENCIES, 9 (Dec. 2018), https://www.gao.gov/assets/700/695981.pdf [https://perma.cc/UQS4-UWDJ].

81 *See* Hiller, *supra* note 11, at 268-277 (describing the cascade of health data from various sources).

82 Carlton Fields, *2018 Was A Record Year in HIPAA Enforcement*, JD SUPRA (Feb. 18, 2019), https://www.jdsupra.com/legalnews/2018-was-a-record-year-in-hipaa-67308 [https://perma.cc/A4HT-RQHT].

83 Lily Hay Newman, *The Covid-19 Pandemic Reveals Ransomware's Long Game*, WIRED (Apr. 20, 2020), https://www.wired.com/story/covid-19-pandemic-ransomware-long-game [https://perma.cc/T55D-Y8GG]; Aaron F.

The exclusion of the individual from critical infrastructure is in direct opposition to data indicating that individuals are often both the unwitting victims and perpetrators of nearly all cyber intrusions.[84] The inability to secure the individual within the digital ecosystem constitutes a recurrent and lasting vulnerability. While multinational corporations, governments, and large existing critical infrastructure providers can in many instances purchase high-end cyberdefensive services, individual citizens are wholly unable to do so at this necessary level.[85] A nation that does not secure this ubiquitous infrastructure from external interference and internal malpractice will be subject to economic instability, political opaqueness, citizen distrust, and the destruction of individual agency.

This is the challenge faced by the NoP framework. In a world in which the proliferation of connective technology pervades every aspect of a person's life, the recognition that the unit of analysis needs to be lowered to the individual level compels a reconceptualization of the role of the state as the guarantor of defense, and new legal and regulatory frameworks. Where once bullets and bombs crossing borders were the principal concern of states, bits and bytes are added to this dynamic in a manner that impacts the safety, security, and stability of societies and their citizens.

B. Life Critical Data and Functions

Advances in technologies that intertwine human subjects and computational devices and sensors necessitate the development of an independent category within critical infrastructure protection. Instead of the NIST approach of categorizing a human as a potential security flaw in the infrastructure mentioned in Part I. B., or an entity that is only a user of the data (the e-utility), in the NoP the individual is constitutive of the connective tissue of the infrastructure itself, because of the intimate connection of sensors, data from the sensors, and decision making based on those sensors, all fundamentally connected to human existence. So as not to identify every data point as part of the NoP infrastructure, however, we propose that the *critical* NoP (CNoP) be defined as when the data collected and/or aggregated through the sensors, or decision made as a result thereof, are applicable to "life critical" functions.[86]

Computer software designers consider a program to be life critical by answering the question, "[i]f it fails, will someone die?"[87] Examples included the failure of software that runs autopilot for an airplane, and a defect in the software that guides self-driving cars. We propose a definition of life critical NoP functions that is inclusive of, but broader than, the computer science use of the term, recognizing

---

Brantly, *The Cybersecurity of Health*, COUNCIL ON FOREIGN RELATIONS (Apr. 8, 2020), https://www.cfr.org/blog/cybersecurity-health, [https://perma.cc/5WG2-ECY8].

[84] *See* X-*Force Threat Intelligence Index*, IBM X-FORCE INCIDENT RESPONSE AND INTELLIGENCE SERVICES (IRIS) (2020), https://www.ibm.com/downloads/cas/DEDOLR3W [https://perma.cc/S6HC-H4PX].

[85] *See generally* Lennart Maschmeyer et al., *A Tale of Two Cybers—How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society*, 17 J. INFO. TECH. & POL. 1 (2020).

[86] On the term "life critical," *see generally* WORKING GROUP, SECURITY TENETS FOR LIFE CRITICAL EMBEDDED SYSTEMS (U.S. DEP'T OF HOMELAND SEC. 2015), https://www.cisa.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf [https://perma.cc/882E-HHV9].

[87] Debates about software reliability for life-critical applications are not new. *See, e.g.*, Ricky W. Butler & George B. Finelli, *The Infeasibility of Quantifying the Reliability of Life-Critical Real-Time Software*, 19 IEEE TRANSACTIONS SOFTWARE ENG'G 3 (1993) (proposing that describing "software reliability is meaningless—software is either correct or incorrect with respect to its specification.").

that life critical failures can be insidious, as well as catastrophic. The focus is not exclusively on personally identifiable data in the NoP, although it is one factor that can contribute to a system being linked to a life critical function. Neither is the focus about whether an individual gave consent to the collection of the information; within a CNoP it is highly unlikely that individuals even know whether the information is being collected. Instead, the focus here centers on whether the NoP affects critical life functions, deserving enhanced protection from threats and vulnerabilities.[88]

Recognizing that categories may overlap,[89] we propose that life critical NoP functions be defined as those that affect fundamental rights and obligations in three areas: citizenship, economic necessities, and personhood. Critical citizenship functions include voting, political speech, and other recognized fundamental rights. While the U.S. and other countries' constitutions are obviously essential to protecting fundamental, critical rights of citizens, the sobering fact is that they are insufficient to secure life critical functions in a NoP. Constitutional protections are often enforced ex post,[90] but protecting the NoP as critical infrastructure seeks to protect citizenship rights ex ante.[91] Furthermore, normally the operation of a NoP will be opaque, therefore making ex post citizen enforcement of rights through legal remedies difficult.[92] Life critical citizenship functions also go beyond the negative rights imbued in the Constitution and include those that affect fundamental citizen decision-making within a democracy; this includes NoP activities that can negatively affect governmental transparency,[93] due process,[94] and ultimately, on a broad scale, diminish citizen trust.

---

88 It should be noted that we do not mean to imply that other aspects of surveillance should not be otherwise regulated or certified, but the focus in this paper is limited to the life critical functions that would categorize the infrastructure as critical to national well-being and security. We also recognize that the definition of life critical functions will require further development, and could be related to human rights jurisprudence. That conversation is beyond the scope of this article, although it is suggested for future research.

89 *See* Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 165 (2015) (noting, "The emphasis on dignity and autonomy within the informational privacy context has distracted courts from informational privacy's more limited underlying interests—the protection of intimate information and political thought."). *See generally* Yael Braudo-Bahat, *Towards a Relational Conceptualization of the Right to Personal Autonomy*, 25 AM. U. J. GENDER, SOC. POL'Y & LAW 111, 115–17 (2017) (reviewing liberal meanings of autonomy); Richard H. Fallon, Jr., *Two Senses of Autonomy*, 46 STAN. L. REV. 875, 876 (1994) (discussing the different meanings of autonomy and noting the argument that "autonomy of speech and thought as necessary for legitimate government").

90 *See* Mila Versteeg, *The Politics of Takings Clauses*, 109 NW. U. L. REV. 695 (2015) (referring to the effectiveness of constitutional anti-takings clauses, and noting that "mechanisms that are supposed to make it harder to deviate from the constitution's promises ex post" can sometimes fail).

91 Ex-ante protection being an essential tenant of Preventive and Proactive Law (PPL). *See* Gerlinde Berger-Walliser et al., *From Visualization to Legal Design: A Collaborative and Creative Process*, 54 AM. BUS. L.J. 347, 364 (2017) (distinguishing PPL from traditional adversary law).

92 *See* Emily Berman, *A Government of Laws and Not Machines*, 98 B.U. L. Rev. 1277, 1322 (2018) (discussing opaqueness as a particular problem for security and law enforcement).

93 *Id.*at 1321.

94 Legal scholarship that analyzes the effect of governmental used algorithms on due process rights is relevant, and addresses one part of the IoP infrastructure, decision making. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1256-58 (2008); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. U. L. REV. 1, 5–6, 18–20 (2014); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 94–101, 121–28 (2014); Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 640, 656 (2017).

Life critical economic necessities encompass, at a minimum,[95] the non-discriminatory employment relationship that underlies a person's ability to earn a living, as reflected in the employment laws that guarantee the right of individuals to engage in non-discriminatory employment opportunities,[96] and access to government support such as employment laws that protect individuals from discriminatory treatment. Yet, the vulnerabilities of employment facing NoP systems could invidiously undermine these rights and poison the market for human capital.

Personhood includes those fundamental rights beyond political citizenship, including autonomy and self-definition. The concept of personhood is closely related to autonomy and the right of an individual to make critical life choices. Autonomy is a recognized, ethical, principle in health care, for example, found in the patient's right to choose treatment options and to make end-of-life decisions.[97]

Applying this concept to the elements of the infrastructure, an e-utility will be a part of the CNoP when it applies a product or service to a critical life function. An example of an e-utility that affects the life critical function of economic necessities would be an employment algorithm that incorporates data collected from where people travel, where they live, how they exercise, and perhaps even what they eat.[98] Human resource professionals have long sought objective ways to make effective, non-discriminatory employment decisions.[99] In recent years, employers and consultants have started incorporating larger sets of data and analytics methods into employment decision-making.[100] As applied

---

95 Economic rights are found more broadly in international documents, yet the adoption of these rights is not consistent worldwide. *See generally* Steven A. Ramirez, *Taking Economic Human Rights Seriously After the Debt Crisis*, 42 LOY. U. CHI. L.J. 713, 715 (2011) ("Economic human rights include, among other rights, the right to be free from discrimination, the right to a basic education, the right to advanced education based upon merit, the right of laborers to pursue collective bargaining, and the right to decent health care and living conditions."). Statutory action may be needed to expand employment rights beyond non-discrimination. Therefore, we leave the question of how far economic rights should extend to another discussion, focusing on the established rights of non-discrimination.

96 *See generally* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016); Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857 (2017).

97 *See* Erin Sheley, *Rethinking Injury: The Case of Informed Consent*, 2015 BYU L. REV. 63, 69–73 (2015) (proposing that informational privacy rights promote the relationship between two premises of medical ethics; autonomy and beneficence, applied to informed consent).

98 Te-Ping Chen, *Your Company Wants to Know if You've Lost Weight*, WALL ST. J. (Feb. 11, 2019, 11:28 AM), https://www.wsj.com/articles/does-your-company-need-to-know-your-body-mass-index-11549902536 [https://perma.cc/KYH3-RR7E].

99 *See also* Alec Levenson, *The Promise of Big Data for HR*, 36 PEOPLE & STRATEGY 22 (2014) (focusing on the experiences of employees once hired). *See generally Big Data in the Workplace: Examining Implications for Equal Employment Opportunity Law*, Meeting of the Equal Employment Opportunity Commission (Oct. 13, 2016) [hereinafter *Trindel*] (statement of Dr. Kelly Trindel, Chief Analyst, Office of Research, Information, and Planning, EEOC), available at https://www.eeoc.gov/meetings/meeting-october-13-2016-big-data-workplace-examining-implications-equal-employment/trindel%2C%20phd [https://perma.cc/S5G7-436J] (outlining the opportunities and future concerns for the use of big tech in employment decision making); *Use of Big Data Has Implications for Equal Employment Opportunity, Panel Tells EEOC*, EEOC (Oct. 13, 2016), https://www.eeoc.gov/newsroom/use-big-data-has-implications-equal-employment-opportunity-panel-tells-eeoc [https://perma.cc/6S4S-W6AC] (highlighting the potential and the problems with big data in the employment context).

100 Mark Feffer, *HR Moves Toward Wider Use of Predictive Analytics* SHRM (Oct. 6, 2014), https://www.shrm.org/ResourcesAndTools/hr-topics/technology/Pages/More-HR-Pros-Using-Predictive-Analytics.aspx [https://perma.cc/5RKS-7D7W]. For a broad description of applications and explanation of terminology, *see Predictive Analytics: What it is and why it matters*, SAS https://www.sas.com/en_us/insights/analytics/predictive-analytics.html (last visited Nov. 1,

to employment-related decision making, the EEOC Office of Research describes such a process as "the combination of nontraditional and traditional employment data with technology-enabled analytics to create processes for identifying, recruiting, segmenting, and scoring job candidates and employees."[101] Sometimes called "people analytics," companies' human resources departments already use data that is collected outside of the workplace to make employment decisions.[102] Multiple sensors that are either worn by or closely connected to employees, collecting and processing information to use in employment contexts, triggering employment decisions, will affect a person's ability to earn a livelihood, and even on a broader scale could affect national security by causing market disruption in the workforce. The utilization of machine learning and artificial intelligence has been demonstrated in numerous instances to result in negative externalities on everything from employment decisions to decisions pertaining to parole and the location of businesses within communities.[103] Further concerns include the intersection of health management and care as the proliferation of patient data allows insurance companies, employers, and care providers to maximize efficiency, at times at the expense of the human subject.[104]

While many negative externalities of decision triggers may be unintentionally programmed in, it is also possible to manipulate them to achieve directed effects. Two principal examples serve to illustrate the potential impact of such manipulations. The first incident occurred in 2013, when the Syrian Electronic Army hacked the AP News Twitter account and posted that President Obama had been injured in a terrorist bombing of the White House.[105] The result of the attack was a precipitous $136 billion decline in the stock market as algorithms immediately responded to the news and began a mass sell-off.[106] The second case is Russia's deliberate manipulation of social media algorithms to foster a robust disinformation campaign that reached more than 120 million Americans in the lead up to the 2016 presidential elections.[107] These well-known examples of terrorist and nation state activities to discredit targeted individuals are intended to escalate disruption of an entire industry or country's economic or political system.

Thus, the vulnerabilities faced within the NoP will impact both the critical life functions of the individual, as well as the society at large. In complex digitally and socially networked environments, severe disruptions, manipulations, alterations, or other malfeasance can result in cascading effects, often

---

2020) [https://perma.cc/V6HQ-R947].

101 Trindel, *supra* note 98.

102 *See* Josh Bersin, *People Analytics: Here with a Vengeance*, FORBES (Dec. 6, 2017, 11:39 AM), https://www.forbes.com/sites/joshbersin/2017/12/16/people-analytics-here-with-a-vengeance/#76dd363932a1 [https://perma.cc/2Q9S-SKH4].

103 *See generally* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2018).

104 *See* Hiller, *supra* note 11, at 269–77 (describing the myriad ways that health data may be shared across different platforms).

105 Max Fisher, *Syrian Hackers Claim AP Hack that Tipped Stock Market by $136 Billion. Is It Terrorism?*, WASH. POST (Apr. 23, 2013, 4:31 PM), https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism [https://perma.cc/PL8F-RUUF].

106 *Id.*; Christopher Matthews, *How Does One Fake Tweet Cause a Stock Market Crash?*, TIME (Apr. 24, 2013), https://business.time.com/2013/04/24/how-does-one-fake-tweet-cause-a-stock-market-crash/ [https://perma.cc/XJ6A-Z2PE].

107 THOMAS RID, ACTIVE MEASURES: THE SECRET HISTORY OF DISINFORMATION AND POLITICAL WARFARE 386 (2020).

referred to as "third order effects."[108] While resilience can be developed within some critical infrastructure sectors due to comprehensive knowledge about the industry and abilities, the heterogenous and diffuse CNoP, comprised of billions of devices, is more akin to epidemiological management.[109] As with the Covid-19 epidemic, strong state interventions are required in an attempt to achieve improved outcomes. The absence of state legal and regulatory capacity to intervene can result in deleterious outcomes.

The CNoP may also be compared to the treatment of cybersecurity within national infrastructure protection because it crosses many sectors. The history of cybersecurity is one that combines government intervention, public and private partnership, international norms, and interstate disagreements and is reflected in some of the regulatory approaches to critical infrastructure protection discussed in the following Part III.[110] In this Part, differing United States and European approaches to critical infrastructure security are explained and then applied to the NoP to analyze how to most effectively protect these ubiquitous, national security, and intimately impactful systems.

III. PROTECTING THE CRITICAL NOP

With increased interdependence in critical infrastructure areas such as banking and financial services, transportation systems, and power supply, as well as cyberattacks targeting domestic infrastructure that originate extraterritorially, critical infrastructure protection has become a growing concern for the global community, requiring international collaboration.[111] At the same time, policymakers on both sides of the Atlantic disagree on how to achieve cyber resilience, as exemplified by their opposing positions on cross-border access to electronic evidence or national security agencies' reach into private people's lives.[112]

This part first discusses the approach to critical infrastructure protection by the United States,

---

108 Herbert Lin, *Operational Considerations in Cyber Attack and Cyber Exploitation*, *in* CYBERSPACE AND NATIONAL SECURITY: THREATS, OPPORTUNITIES, AND POWER IN A VIRTUAL WORLD (Derek S. Reveron ed., 2012).

109 Aaron F. Brantly, *Public Health and Epidemiological Approaches to National Cybersecurity: A Baseline Comparison*, *in* U.S. NATIONAL CYBERSECURITY: INTERNATIONAL POLITICS, CONCEPTS AND ORGANIZATION (Damien Van Puyvelde & Aaron F. Brantly eds., 2017).

110 *See* Raluca Bunduchi, et al., *Between public and private – the nature of today's standards* (Aug. 25, 2004) (presented at Standards, Democracy and the Public Interest workshop); WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION (1998); Anders Henriksen, *The end of the road for the UN GGE process: The future regulation of cyberspace,* 5 J. CYBERSECURITY 1, 1–9 (2009). *See generally* DAMIEN VAN PUYVELDE & AARON F. BRANTLY, CYBERSECURITY: POLITICS, GOVERNANCE AND CONFLICT IN CYBERSPACE (2019); Samantha Bradshaw et al., *The Emergence of Contention in Global Internet Governance*, GLOB. COMM'N ON INTERNET GOVERNANCE (2015)

111 *See* JING DE JONG-CHEN & BOBBY O'BRIEN, A COMPARATIVE STUDY: THE APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION IN THE U.S., E.U., AND CHINA 11 (2017), https://www.wilsoncenter.org/sites/default/files/media/documents/publication/approach_to_critical_infrastructure_protection.pdf [https://perma.cc/RCA8-UJR5] (recommending global collaboration to protect critical infrastructure); *see also* Antonio Segura Serrano, *Cybersecurity: towards a global standard in the protection of critical information infrastructures*, 6 EUROPEAN J.L. & TECH. 1, 2–3 (2015) (citing to international initiatives to strengthen cybersecurity and CIP such as the 2003 G8 Principles for Protecting Critical Information Infrastructures, United Nations General Assembly Resolution 58/199 and 64/211, 2008 OECD Recommendation of the Council on the Protection of Critical Information Infrastructures and 2015 Recommendations on Digital Security Risk Management, and ITU Global Cybersecurity Agenda).

112 *See infra* Part III.B.

and then compares the differing approach by the European Union. The two views of how to protect critical infrastructure are then applied to an analysis of how to most effectively protect a sensitive NoP infrastructure that is centered on persons as opposed to things and how to do so in an internationally coherent way.

A. Critical Infrastructure Protection in the United States

The Critical Infrastructure Protection Act of 2001 defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[113] Representative Thompson explained that "[t]he definition attempts to strike a balance: to not be so vague as to include any infrastructure in the United States (such as a short bridge connecting two small islands of no strategic value), nor so rigid that, as new risks develop or evolve, the definition would become an obstacle to security efforts."[114] Because of the built-in flexibility, it could be argued there is a lack of a clear definition of what constitutes an asset, system, or network.

The U.S. Department of Homeland Security (DHS) states:

> The nation's critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family.[115]

Sixteen sectors are presently classified as critical infrastructure: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation; and water and wastewater.[116] While the DHS has overall leadership of critical infrastructure protection, specific government agencies have jurisdiction to lead particular sectors.[117]

---

113 42 U.S.C. § 5195c(e).

114 Representative Bennie G. Thompson, *A Legislative Prescription for Confronting 21st-Century Risks to the Homeland*, 47 HARV. J. ON LEGIS. 277, 284 (2010).

115 Homeland Security Act of 2002, Pub. L. No. 107–296, 166 Stat. 2135 (codified as amended in 6 U.S.C.); *Sector Risk Management Agencies*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/sector-risk-management-agencies [https://perma.cc/LY8N-QMTB] (last visited Nov. 1, 2020); *see also* Critical Infrastructure Protection Act of 2001, 42 U.S.C. § 5195c(e).

116 *Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Oct. 21, 2020), https://www.cisa.gov/critical-infrastructure-sectors [https://perma.cc/FTK3-RW9T].

117 The White House Off. of the Press Sec'y, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*, OBAMA WHITE HOUSE (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [https://perma.cc/5UAQ-66KS]. DHS states that there are twenty-two federal agencies involved in critical infrastructure protection. *See Homeland Security Enterprise*, U.S. DEP'T HOMELAND SEC. (Oct. 22, 2021), https://www.dhs.gov/topic/homeland-security-enterprise [https://perma.cc/E9MU-RAGU] (discussing the importance of bringing together the government and commercial entities to accomplish shared goals related to critical infrastructure

In the United States, critical infrastructure protection is based on bringing together both the public and private sectors in order to create norms of behavior, sharing vulnerabilities and threats, information, best practices, and planning for resiliency.[118] The voluntary, public-private partnership approach to protecting critical infrastructure is a result of years of Presidential Directives across multiple administrations and a few legislative actions between 1996 and 2003.[119] Major elements of critical infrastructure protection, focusing on those most relevant to the discussion, include a National Infrastructure Protection Plan,[120] a Strategy to Secure Cyberspace,[121] Sector Specific Agencies[122] for coordination, and Information Sharing and Analysis Organizations.[123] The National Cybersecurity Protection Act[124] created the National Cybersecurity and Communications Integration Center (NCCIC),[125] later falling under the jurisdiction of the Cybersecurity and Infrastructure Security Agency (CISA). CISA and its sub-units provide the resources and leadership for public-private sector information sharing.[126]

DHS promotes a risk management approach for the protection of critical infrastructure.[127] It

---

protection).

118 *See* U.S. DEP'T OF HOMELAND SEC., NIPP 2013: PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE 10–12 (2013), https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf [https://perma.cc/W2FV-E9HD].

119 *See* Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 FLA. ST. U. L. REV. 515, 525–31 (2017) (discussing Presidential Directives related to critical infrastructure protection up until 2013); Joe D. Whitley et al., *Homeland Security, Law, and Policy Through the Lens of Critical Infrastructure and Key Asset Protection*, 47 JURIMETRICS 259, 261–63, 2007 (reviewing a series of Presidential Directives and Homeland Security Directives between 1996 and 2003).

120 U.S. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN: PARTNERING TO ENHANCE PROTECTION AND RESILIENCY (2009), https://files.eric.ed.gov/fulltext/ED507739.pdf [https://perma.cc/NAP7-Z34G].

121 There have been multiple iterations of a national strategy, beginning with the 2003 version, and each primarily adopts a voluntary collaborative role with the private sector and a limited regulatory approach. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, THE NATIONAL STRATEGY TO SECURE CYBERSPACE ix (2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf [https://perma.cc/GX75-KL9Y] ("In general, the private sector is best equipped and structured to respond to an evolving cyber threat."). The most recent strategy was issued in 2018, confirming the expectation that market forces will enable cybersecurity efforts. EXEC. OFF. OF THE PRESIDENT, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 14 (2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [https://perma.cc/S23F-36YQ] ("To enhance the resilience of cyberspace, the Administration expects the technology marketplace to support and reward the continuous development, adoption, and evolution of innovative security technologies and processes.").

122 *2015 Sector-Specific Plans*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/2015-sector-specific-plans [https://perma.cc/73GU-UHZB].

123 Exec. Order No. 13691, 80 Fed. Reg. 9,349 (Feb. 20, 2015).

124 National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066 (2014) (codified as amended at 6 U.S.C. §§ 101, 148-50).

125 *Id.*

126 Cybersecurity Act of 2015, Pub. L. 114–113, 129 Stat. 2935 (2015) (codified as amended at 6 U.S.C. § 1501). Act is referred to in § (c)(3) Div. N. For complete classification of this Act to the Code, see § 101, 6 U.S.C. § 1501. This chapter, referred to in § (c)(7) and § (e)(1)(J), was in the original "this Act," meaning Homeland Security Act of 2002, Pub. L. 107–296, 116 Stat. 2135, which is classified principally to this chapter.

127 DEP'T HOMELAND SEC., SUPPLEMENTAL TOOL: EXECUTING A CRITICAL INFRASTRUCTURE RISK MANAGEMENT APPROACH, (2013), https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-

integrates "physical, cyber, and human elements"[128] within the risk management framework that includes a process of adopting goals and objectives within an infrastructure, assessment and analysis of risks, risk management actions, and evaluation of effectiveness, in an iterative process.[129] Thus, the DHS approach does not segment "cyber elements of critical infrastructure," but includes them as integrative parts of other infrastructures and business operations that should nonetheless be treated uniquely within the risk management process.[130] In this light, DHS focuses primarily on Internet communications but also engages in "Cyber-Dependent Infrastructure Identification" with agencies and partners.[131] It is fair to note that the Internet environment has changed drastically since 2013, and the risk management approach may in practice look drastically different today as applied to a ubiquitous system of data collection.[132]

As part of its continuing work, in 2016, DHS published Strategic Principles for Securing the Internet of Things (IoT), noting that "[b]ecause our nation is now dependent on properly functioning networks to drive so many life-sustaining activities, IoT security is now a matter of homeland security."[133] The lack of even fundamental security in IoT devices led the DHS to lay fault at the lack of clear obligations in the supply chain, together with the absence of norms, incentives, and awareness.[134] Consequently, DHS proposed the incorporation of security principles of security by design, updates and vulnerability patches, best practices, a risk management approach, transparency, and care in connectivity, directed at developers, manufacturers, service providers, and "business-level consumers."[135]

The U.S. voluntary public-private partnership approach, rather than a top-down regulatory one, is premised in part on the fact that the majority of the critical infrastructure, including networks, are privately owned, that technology is fast-moving, and that the market will respond to the need for security most efficiently.[136] The Cybersecurity Risk Management Framework,[137] a voluntary standard set by the NIST, has had some success establishing norms of security behavior.[138] Some criticism of

---

Mgmt-Approach-508.pdf [https://perma.cc/B2E2-TMDZ] (part of the NIPP).

128 *Id.* at 2.

129 *Id.*

130 *Id.* at 5.

131 *Id.*

132 *Id.* at 1. The steps include: "1. Set Goals and Objectives, 2. Identify Infrastructure, 3. Assess and Analyze Risks, 4. Implement Risk Management Activities, 5. Measure."

133 DEP'T HOMELAND SEC., STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IOT), 2 (Nov. 15, 2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf [https://perma.cc/BKL8-GNML].

134 *Id.* at 3.

135 *Id.* at 3–4.

136 *See* John J. Chung, *Critical Infrastructure, Cybersecurity, and Market Failure*, 96 OR. L. REV. 441, 464–69 (2018) (describing benefits of a voluntary partnership with the private sector).

137 *See* Voas, *supra* note 34.

138 *Department of Commerce Launches Collaborative Privacy Framework Effort*, NAT'L INST. STANDARDS & TECH., U.S. DEP'T OF COMMERCE (Sept. 4, 2018), https://www.nist.gov/news-events/news/2018/09/department-commerce-launches-collaborative-privacy-framework-effort [https://perma.cc/G3KF-L3GK].

(stating that the success of the Cybersecurity Framework has provided guidance in developing the Privacy Framework)*; see also* Jordan M. Blanke, *Top Ten Reasons to Be Optimistic About Privacy*, 55 IDAHO L. REV. 281, 292 (2019); Jordan M. Blanke & Janine S.

the market-driven, voluntary approach is that it is too weak and ineffective to protect critical infrastructure from threats at a proactive level.[139]

Scholars Haber and Zarsky articulate a broad analysis of the arguments for and against a primarily voluntary approach to cybersecurity protection for critical infrastructure protection.[140] The interrelated, but unique, points of debate identified are: reliance on the market based approach, impact of disclosure and information sharing, and the effects of externalities.[141] While theory would indicate that consumers will move the needle towards security protection by signaling their preference for such in the market, Haber and Zarsky argue that the non-competitive nature of many markets, and consumers' lack of complete information about cyber security threats and protective measures, serve to dilute the power of the market to produce protective actions.[142] Second, negative externalities occur because of the very nature of the network effect of cyber vulnerabilities, as "[t]he aggregate social harm of a successful critical infrastructure cyber attack will most likely be higher than the aggregate harm to both the firm and its consumers."[143] In response, it is unlikely that a company would take responsibility for this broader range of impacts. Lastly, the fast changing nature of cyber threats and increasing sophistication of bad actors create a challenging environment for individual companies, and as a result they often lag behind in their knowledge and ability to provide an effective defense.[144] Information-sharing between companies, and between companies and governments, is fraught with disincentives for sharing because of lack of trust and fear of liabilities.[145] In sum, Haber and Zarsky argue that there are reasons to consider a stronger regulatory approach to protecting cyber critical infrastructures.[146] As these arguments may apply to the protection of a NoP, they are revisited in Part C.

B. Critical Infrastructure Protection in the European Union

While key strategies and goals are similar, critical infrastructure protection implementation in the European Union significantly differs from the U.S. approach.[147] In contrast to the United States'

Hiller, *Predictability for Privacy in Data Driven Government*, 20 MINN. J.L. SCI. & TECH 32, 42 (2019).

139 *See* Chung, *supra* note 135, at 469–472; Robert S. Metzger, *Security and the Internet of Things*, 14 ABA SCITECH LAW, 4, 7 (2018) ("The risks of trusting 'market driven' solutions will be unacceptable where dependency on the IoT creates serious risk to critical infrastructure or national security"); Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1507–08 (2017) ("Many companies that operate critical infrastructure tend to underinvest in cyber-defense because of negative externalities, positive externalities, free riding, and public goods problems. . . .").

140 *See generally* Haber & Zarsky, *supra* note 118.

141 *See generally id.* at 542–57 (analyzing these three different regulatory strategies and their systematic shortcomings).

142 *Id.* at 544–46.

143 *Id.* at 547.

144 *Id.* at 548.

145 *Id.*

146 *See generally id.* at 550–59 (explaining that in light of disclosure requirements, information gaps, and externalities, a government centered approach has advantages).

147 *See* AEGIS, WHITE PAPER ON CYBERSECURITY POLICY: COMMON GROUND FOR EU-US COLLABORATION 6 (2019) https://aegis-project.org/wp-content/uploads/2019/01/AEGIS-White-Paper-on-Cybersecurity-Policy.pdf [https://perma.cc/2LGS-WE4R] (attributing the differences in part to "the layers of agencies and processes the US involves in cybersecurity as well as the willingness of the respective legislative bodies to pass regulations").

voluntary approach to critical infrastructure protection,[148] in large part, EU regulation focuses on certain areas of critical infrastructure protection, but makes protection in these areas mandatory for European critical infrastructure operators.[149] While the U.S. regime is frequently described as a public-private partnership, European critical infrastructure protection—as argued below—can be qualified as a fully integrated corporate regulatory feedback loop.[150] Further, as a top-down approach, the EU regime is said to be "more streamlined" than the fragmented result of years of presidential directives in the United States.[151] However, the national laws of the individual member states supplement EU law, and EU Directives intentionally provide only a minimum standard and the requirement of transposition into national law.[152] According to the preamble of the EU-Directive on European Critical Infrastructures (ECI Directive), "[i]t is up to each Member State to decide on the most appropriate form of action with regard to the establishment of [critical infrastructure operator security plans]."[153]

Three points of EU critical infrastructure protection are relevant for comparison. A concerted European policy on critical infrastructure emerged in 2004, with an official communication by the European Commission as a response to terrorism threats.[154] Subsequently, the European Programme of Critical Infrastructure Protection was established in 2006[155]—including the ECI Directive from 2008—which provides the overall legal framework for critical infrastructure protection in the European Union, and is the first point of comparison.[156] The directive applies exclusively to the energy and transportation sector, obliging owners or operators of critical infrastructure in these sectors to prepare security plans and nominate so-called security liaison officers who will cooperate with the national

---

148 Defining it as "sectors that compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." *See* DEP'T HOMELAND SEC., *supra* note 126 (and accompanying text).

149 *See* Serrano, *supra* note 110, at 5 (citing to and stating that Exec. Order No. 13, 636, § 2 together with PPD-21 "offer[] a very large concept of 'critical infrastructure'").

150 The concept of CRFLs is described in Stephen K. Park & Gerlinde Berger-Walliser, *A Firm-Driven Approach to Global Governance and Sustainability,* 52 AM. BUS. L.J. 255, 289 (2015).

151 *See* AEGIS, *supra* note 146, at 5.

152 The EU-Directive on European Critical Infrastructures [hereinafter ECI Directive] in section 6 to the preamble of the directive states that "[t]he primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures." Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, 2008 O.J. (L 345/75), pmbl. § 6. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114 [https://perma.cc/4PMR-E6GU] [hereinafter ECI Directive]. Section 10 reads: "[t]his Directive complements existing sectoral measures at Community level and in the Member States. Where Community mechanisms are already in place, they should continue to be used and will contribute to the overall implementation of this Directive. Duplication of, or contradiction between, different acts or provisions should be avoided." *Id. at* § 10.

153 *Id.* at § 6.

154 *See Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the Fight Against Terrorism*, COM (2004) 0702 final (Oct. 20, 2004), https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:52004DC0702 [https://perma.cc/6TGN-8XYQ]GL8K-UAPD].

155 *See Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection*, COM (2006) 786 final (Dec. 12, 2006), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33260&from=EN [https://perma.cc/H3AG-96J2].

156 ECI Directive, *supra* note 151.

authorities responsible for critical infrastructure protection in the given member state.[157] Due to the European Union's political structure as a union of sovereign states, the EU directive combines preventative measures and reaction to threats with coordination requirements between member states. There is no EU-wide regulation for other sectors that would be considered critical under the DHS definition.[158]

The second significant critical infrastructure protection component in the European Union, the Network and Information Security Directive (NIS Directive), was adopted in 2016 and is broader.[159] The NIS Directive supplements the ECI Directive and it establishes an entity that can be regarded as the European equivalent to NIST. The NIS Directive harmonizes cybersecurity and notification requirements for "operators of essential services" (OESs)—the European equivalent to critical service providers in the United States—across European member states.[160]

The third leg of critical infrastructure protection in the European Union is related to its well-known laws and policies governing privacy and data protection, exemplified by its recent enactment of the General Data Protection Regulation (GDPR).[161] Furthermore, some European countries' constitutions, such as the German Basic Law, include an individual right to the guarantee of confidentiality and integrity of information technology systems, which must be carefully balanced against the state's interest in protecting critical infrastructure.[162]

The following sections discuss these three prongs of critical infrastructure protection in the European Union as an example for an alternative approach to the current U.S. critical infrastructure protection in a similarly developed, technologically-driven market economy.[163]

---

157 *See* ECI Directive, *supra* note 151, arts. 3, 5–6.

158 *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Dec. 17, 2003), https://www.cisa.gov/homeland-security-presidential-directive-7 [https://perma.cc/8G5J-X4MU].

159 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC [https://perma.cc/S9PY-JQ69] [hereinafter NIS Directive].

160 NIS Directive, art. 5 § 2 defines operators of essential services as "(a) an entity [that] provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service."

161 Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR]. *See also* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 877 (2014) ("In the United States, privacy law focuses on redressing consumer harm and balancing privacy with efficient commercial transactions. In the European Union, privacy is hailed as a fundamental right that can trump other interests.").

162 *See generally,* Bundesverfassungsgereicht [BVerfG] [Constitutional Court] Feb. 27, 2008, 120 BVERFG 274 (Ger.) (For English version, *see* https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html [https://perma.cc/VF9U-CA79]).

163 *See* Serrano, *supra* note 110, at 1 (suggesting that the United States and the European Union are among the first countries that have adopted important cybersecurity regulation).

1. ECI Directive

The ECI Directive "establishes a procedure for the identification and designation of European critical infrastructures ('ECIs'), and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people."[164] At first sight, the EU directive's definition of critical infrastructure is similar to that of the U.S. DHS.[165] However, the slight differences in wording are telling of the different approaches to the role of the individual within U.S. and EU critical infrastructure protection: according to the EU directive,

> 'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.[166]

Remarkably, EU critical infrastructure – contrary to the DHS's definition – is not limited to "security, national economic security, national public health or safety,"[167] but includes the "social well-being of people."[168] This definition puts the person right at the center of critical infrastructure protection and expressively includes the protection of "vital societal functions."[169]

According to the directive, infrastructure qualifies as "critical" if it meets the so-called "cross-cutting criteria threshold."[170] The directive defines these criteria as follows:

> (a) casualties criterion (assessed in terms of the potential number of fatalities or injuries);
>
> (b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services, including potential environmental effects);
>
> (c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life, including the loss of essential

164 ECI Directive, art. 1.

165 *See* Eimear Bourke, *A War Without Bullets: Protecting Civilians in the Technology Trenches*, 28 ALB. L.J. SCI. & TECH. 1, 5 (2018) (comparing EU and U.S. definition of critical infrastructure and qualifying them as "similar").

166 ECI Directive, art. 2 § (a).

167 *See* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *supra* note 114 (defining critical infrastructure as "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof").

168 ECI Directive, art. 2 § (a).

169 *Id.*

170 ECI Directive, art. 3 §§ 1 – 2.

services).[171]

The threshold applicable to the cross-cutting criteria is "based on the severity of the impact of the disruption or destruction of a particular infrastructure."[172] When this level is reached is "determined on a case-by-case basis by the Member State."[173] The directive obliges member states to identify ECIs that meet the directive's criteria, and the European Commission may assist member states in this task.[174] Operators or owners of ECIs are defined as "entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive."[175] Designated ECI operators must appoint a security liaison officer, who communicates and collaborates with the national critical infrastructure authorities.[176] They are further required to set up operator security plans or "equivalent measures" that identify "important assets, a risk assessment and the identification, selection and prioritisation of counter measures and procedures."[177] Each member state of the European Union must ensure that operator security plans are in place and determine appropriate measures where "such plans do not exist[]."[178]

In addition to measures targeting ECI operators, the directive aims to improve efficiency in communication among different actors in critical infrastructure protection, namely ECI operators/owners, national authorities, the scientific community, and EU authorities. To do so, the directive requires member states to appoint "European critical infrastructure protection contact points" that "coordinate European critical infrastructure protection within the Member State, with other Member States and with the [European] Commission."[179] The European Programme of Critical Infrastructure Protection has established the European Reference Network for Critical Infrastructure Protection, which "provid[es] a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards."[180]

---

171 *Id.*

172 *Id.*

173 *Id.*

174 ECI Directive, art. 3 § 1.

175 ECI Directive, art. 1 § (f).

176 *See* ECI Directive, pmbl. § 13 (specifying that "[w]here such a Security Liaison Officer does not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place. It is up to each Member State to decide on the most appropriate form of action with regard to the designation of Security Liaison Officers.").

177 *See* ECI Directive, art. 5 ("The minimum content to be addressed by an ECI OSP procedure is set out in Annex II" of the directive).

178 *See* ECI Directive, pmbl. § 11.

179 ECI Directive, art. 10 § 1, 2.

180 EU SCIENCE HUB, https://ec.europa.eu/jrc/en/network-bureau/european-reference-network-critical-infrastructure-protection-erncip_(last visited Oct. 31, 2020). [https://perma.cc/T4AK-S6ZN]. Hence, the directive establishes both obligations for ECI operators towards their governments on the one hand, and member states' obligations towards other countries and the community on the other. Owners or operators of ECI, however, are expected to primarily with their respective national authorities, not directly with the European Union. *See* ECI Directive, pmbl. § 16 ("Owners/operators of ECIs should be given access primarily through relevant Member State authorities to best practices and methodologies concerning critical infrastructure protection."). This reflects the fundamental EU policy principle of subsidiarity, which assumes that issues are best handled on the local level unless effective protection by reason of scale can better be achieved through a common EU-wide

The three-tier collaboration established by the directive creates a system of corporate regulatory feedback loops (CRFLs) between mostly private operators/owners of ECI and national government entities on the one hand, and national governments and the European Commission on the other hand. In general, a feedback loop is "a cycle that is comprised of output from, or information about the result, of phenomena that causally influences other phenomena within the cycle and perpetuates the phenomena as a circuit or loop that feeds back into itself."[181] Previously, CRFLs have been suggested as a policy instrument to enhance the legitimacy and efficiency of corporate sustainability rulemaking.[182] Transposed to European critical infrastructure protection, CRFLs can be described as processes of social interaction between an operator/owner of ECI and governmental entities (including both regulatory bodies and nonregulators) that enhance the visibility, identification, and internalization of threats and risks to ECI, as well as costs and potential mutual benefits of European critical infrastructure protection.[183] The ECI Directive, through its system of continuous, institutionalized interactions among ECI operators, national governments, the European Programme of Critical Infrastructure Protection, and community government, harnesses the power of such feedback loops by sequentially linking a series of responsive actions to threats to the ECI.[184]

In this regard, the European critical infrastructure protection differs from the mostly voluntary system in the United States, while preserving the flexibility and efficiency commonly attributed to voluntary regulatory regimes and public-private partnerships.[185] Through their interactions with democratically legitimate government bodies, CFRLs force private actors to "take into account shared public values and stakeholder interests."[186] Hence, the European critical infrastructure protection's embedded regulatory feedback loops are better suited to take into account societal values, such as securing democracy and protecting a person's fundamental rights than a substantially voluntary public-private partnership. Respect of these or other stakeholder concerns may be missing in a private system that focuses on securing the infrastructure for more limited economic or national security reasons.

---

approach. *See* ECI Directive, pmbl. § 20. Accordingly, under the directive, individual member states have the responsibility to guarantee the flow of information from the community to the operators of ECI, and vice-versa. *See* ECI Directive, pmbl. § 14 ("Each Member State should collect information concerning ECIs located within its territory. The Commission should receive generic information from the Member States concerning risks, threats and vulnerabilities in sectors where ECIs were identified. . . ."). In 2018, the Commission launched an evaluation to assess the directive's effectiveness and published the results on the Commission's website. *See* EVALUATION OF THE 2008 EUROPEAN CRITICAL INFRASTRUCTURE PROTECTION DIRECTIVE, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1631-Evaluation-of-the-2008-European-Critical-Infrastructure-Protection-Directive (last visited Oct. 31, 2020). [https://perma.cc/B3TB-SRQN].

181 *See* Keith Aoki et al., *Pastures of Peonage: Tracing the Feedback Loop of Food Through IP, GMOs, Trade, Immigration, and U.S.*, Agro-Maquilas, 4 NE. U. L. J. 1, 4 n.6 (2012) (defining feedback loops).

182 Park & Berger-Walliser, *supra* note 149, at 291.

183 *Id.* at 290–91.

184 ECI Directive, pmbl. § 14 provides: "Each Member State should collect information concerning ECIs located within its territory. The Commission should receive generic information from the Member States concerning risks, threats and vulnerabilities in sectors where ECIs were identified, including where relevant information on possible improvements in the ECIs and cross-sector dependencies, which could be the basis for the development of specific proposals by the Commission on improving the protection of ECIs, where necessary."

185 *See* Park & Berger-Walliser, *supra* note 149, at 277 ("[Soft law's] inherently informal, open-ended nature is the source of its comparative advantage. The speed and flexibility of soft law often makes it easier to create.").

186 *Id.* at 291.

2. NIS Directive

The second leg of European critical infrastructure protection is the more recent NIS Directive from 2016. The directive is part of a wider European cybersecurity strategy,[187] which "stresses that EU's core values apply as much in the digital as in the physical world, including the protection of fundamental rights, freedom of expression, personal data and privacy, and access for all."[188] Hence, privacy, data protection and cybersecurity are all part of a common policy. It is beyond the scope of this article to describe EU cybersecurity policy in detail.[189] Accordingly, the following analysis will concentrate on areas where cybersecurity and critical infrastructure protection overlap, especially as they relate to the CNoP. It will discuss other issues only to the extent necessary for a general understanding of the NIS Directive and later the General Data Protection Regulation.

The NIS Directive is at the core of the EU legal framework for cybersecurity. Recognizing that network and information systems play a vital role in the European economy and society, the directive harmonizes cybersecurity and notification requirements for "operators of essential services" (OESs)—the European equivalent to critical service providers—across European member states as well as digital service providers (DSPs)—a difference that will be discussed in more detail below.[190] According to the directive, an OES is an entity that "(a) . . . provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) . . . depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service."[191] OESs are required to notify the authorities "of incidents having a significant impact on the continuity of the essential services they provide" in a timely manner.[192] Moreover, they must have a "state of the art" risk management system in place that "ensure[s] a level of security of network and information systems appropriate to the risk posed."[193] It is up to the member states to identify OESs in the following sectors: energy, transportation, banking and financial services, health, drinking water, and digital infrastructure.[194]

While the NIS Directive, contrary to the NIST framework, establishes mandatory requirements for OESs and—to a more limited extent—DSPs, the NIS Directive, just like NIST, does not tell OESs what measures they must take to demonstrate compliance.[195] However, according to the

---

187 *See generally Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, COM (2013) 1 final (Feb. 7, 2013).

188 Serrano, *supra* note 110, at 8.

189 This has been done expertly in Scott J. Shackelford & Scott Russell*, Operationalizing Cybersecurity Due Diligence: A Transatlantic Case Study*, 67 S.C. L. REV. 609 (2016) (comparing U.S. and EU cybersecurity due diligence). *See also* U.S. CHAMBER OF COMMERCE, TRANSATLANTIC CYBERSECURITY: FORGING A UNITED RESPONSE TO UNIVERSAL THREATS 20 (2017), https://www.uschamber.com/TransatlanticCybersecurityReport [https://perma.cc/ZV8E-WED7] [hereinafter Transatlantic Cybersecurity] (providing a comprehensive overview of EU cybersecurity frameworks).

190 NIS Directive, art. 1 § (d).

191 NIS Directive, art. 5 §§ (1)–(2) (outlining the criteria for identification of OESs).

192 NIS Directive, art. 14 § (3). The sectors to which the requirements apply are enumerated in Annex II of the directive.

193 *Id.* § (1).

194 After its entry into force, the directive required member states to identify OESs by November 9, 2018. NIS Directive, art. 5 § (1). The sectors concerned are listed in Annex II.

195 AEGIS, *supra* note 146, at 9. The goal of both frameworks is to keep cybersecurity risk management systems adaptable to rapid change, or, in the words of NIS Directive, "state of the art." NIS Directive, art. 14 § (1)*; see also* Transatlantic

directive, "Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems."[196] This reference to international standards represents a unique chance for the development of an internationally harmonized cyber-risk management system that the U.S. Cybersecurity Enhancement Act of 2014 also calls for.[197] Increased reliance on international standards might also open the door to the development of a legally enforceable international standard of cybersecurity care across critical infrastructures.[198]

Like any directive, the NIS Directive does not apply directly to the private companies that it regulates.[199] EU member states were under the obligation to transpose the Directive into national law by May 2018.[200] In addition to the requirements imposed on service providers, the Directive requires member states to develop a national NIS strategy, and they must establish a Computer Security Incident Response Team, as well as a national NIS authority.[201]

For the purpose of this article, the most interesting feature of the NIS Directive, however, is that it does not only apply to critical services providers also covered by NIST, but includes "digital service providers" (DSPs) that are not necessarily critical providers.[202] DSPs are private companies that provide information society services by electronic means at the individual request of a recipient of services,[203] such as online marketplaces, online search engines, and cloud computing services.[204] While the internet's importance as critical infrastructure for national defense, energy, finance, transportation, and fundamental life functions has been largely recognized, DSPs—at least in the United States—have

---

Cybersecurity, *supra* note 188, at 27.

196 NIS Directive, art. 19 § (1).

197 *See* Nizan Geslevich Packin*, Too-Big-to-Fail 2.0? Digital Service Providers as Cyber-Social Systems*, 93 IND. L.J. 1211, 1231 (2018) ("The Cybersecurity Enhancement Act of 2014 directed NIST to coordinate American agencies to work with other jurisdictions to create international cybersecurity principles."). For a comparison of NIST framework, GDPR, and NIS Directive, *see* Transatlantic Cybersecurity, *supra* note 188, at 20.

198 *See* Shackelford & Russell, *supra* note 188, at 618 ("[T]he NIST Framework 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 a number of nations. . . .").

199 EU regulations are directly binding without additional domestic legislation, while EU directives require local legislation in each member state. *See* European Union, *Regulations, Directives and Other Acts*, EUROPA, https://europa.eu/european-union/law/legal-acts_en [https://perma.cc/6WY4-PJL2].

200 NIS Directive, art. 25.

201 NIS Directive, arts. 7–10.

202 A distinction that is not unproblematic. *See generally* Steve Ritter & Laura Schulte, *Rechtliche Anforderungen an Anbieter digitaler Dienste, die zugleich kritische Infrastrukturen sind*, 35 COMPUT. & RECHT 617 (2019) (Ger.).

203 *See* NIS Directive, art. 4 § (5) (referencing "Directive (EU) 2015/1535 of the European Parliament and of the Council" "laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services"); NIS Directive, art. 1 § (1)(b) (defining Information Society service as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.").

204 NIS Directive, Annex III. The Directive restricts DSPs to these three categories. Providers of other categories of digital services such as streaming, online gaming, or social network providers are not included. *See* Jones Day, *The New EU Cybersecurity Directive: What Impact on Digital Service Providers?*, JONES DAY INSIGHTS (Aug. 2016), https://www.jonesday.com/en/insights/2016/08/the-new-eu-cybersecurity-directive-what-impact-on-digital-service-providers [https://perma.cc/F9L8-KRLM] (mentioning that inclusion of these DSPs was debated during the legislative process but were ultimately left out of the Directives).

received far less regulatory attention.[205] Their inclusion in the NIS Directive was not without opposition during the legislative process.[206] This explains the limitation to only three categories of DSPs, and it led to lighter requirements regarding their "state of the art" risk management processes and notification requirements than those required for OESs.[207]

With the move towards a CNoP and its dependence on big data, DSPs, at least in certain categories, such as cloud computing services that store or process the data, become increasingly important for the maintenance of critical societal and/or economic activities. If medical decisions or police action in real time depend on these services, disruption of, or an attack against them, could have a severe effect on life critical functions and ultimately deprive people of their fundamental rights or lead to death. Hence, it can and should be argued that these DSPs are in fact critical service providers and should be treated as such.

3. Data Privacy and Security

The diverging approaches to privacy and data protection between the U.S. and the EU are explained by fundamentally different constitutional underpinnings for privacy protection in general, and data privacy specifically, on both sides of the Atlantic. The constitutional characteristics, in turn, can be attributed to historic developments that, in the aftermath of World War II in Europe, led to the enactment of the European Convention for the Protection of Human Rights and Fundamental Freedom (ECHR). The ECHR, in Article 8, establishes a fundamental right to "respect for private and family life."[208] This has since been interpreted to encompass a fundamental right to protection of personal data.[209] In Europe, privacy is understood as an expression of human dignity that is inviolable and that the state has an obligation to protect.[210] The Charter of Fundamental Rights of the European

---

205 *See* Geslevich Packin, *supra* note 196, at 1243 (describing the internet's role as critical infrastructure); *id.* at 1232 (explaining that this regulatory oversight may be caused by "the lack of support from the private sector" and the fact that "while many believe that major attacks will happen soon, cyberattacks in the United States have not resulted in death or drastic damage to national security or the economy thus far").

206 *See* Jones Day, *supra* note 203 (stating that "opponents viewed cyberattacks on [DSPs] as insufficiently significant and therefore argued against additional regulation, which would potentially negatively affect innovation").

207 NIS Directive, art. 16; *see also id.* pmbl. (stating that "the security requirements for digital service providers should be lighter.").

208 The European Convention for the Protection of Human Rights and Fundamental Freedoms states in Article 8: "Everyone has the right to respect for his private and family life . . . [t]here shall be no interference. . . ." European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, https://www.echr.coe.int/documents/convention_eng.pdf [https://perma.cc/2L7V-BLQD]. Given its historical experience with widespread surveillance during the Third Reich and later under the socialist regime in East Germany, it should come as no surprise that the first Data Protection Act was passed in Germany. *See* Eric Caprioli et al., *The Right to Digital Privacy: A European Surv*ey, 3 RUTGERS J. L. & URB. POL'Y 211, 213 (2006) (referencing the first Data Protection Act passed by the West German Land of Hesse in 1970). This law already introduced the data protection officer, which is now mandated in GDPR art. 37.

209 *See* MARCUS HEINEMANN, GRUNDRECHTLICHER SCHUTZ INFORMATIONSTECHNISCHER SYSTEME: UNTER BESONDERER BERÜCKSICHTIGUNG DES GRUNDRECHTS AUF GEWÄHRLEISTUNG DER VERTRAULICHKEIT UND INTEGRITÄT INFORMATIONSTECHNISCHER SYSTEME 225 (2015) (Ger.).

210 *See* EU Charter of Fundamental Rights of the European Union, Art. 1, 2000 O.J. (C 364) 9 [hereinafter ECFR], https://www.europarl.europa.eu/charter/pdf/text_en.pdf [https://perma.cc/9E99-8A8H]. *See generally* James Q. Whitman, *The*

Union from 2000 and Article 16(1) of the Treaty on the Functioning of the European Union further provide a specific data protection right to citizens in the European Union.[211] The GDPR and its predecessor directive are outgrowths of this fundamental EU right to data protection by the European governments.[212] In the European Union, the implication of personal data of any kind triggers the application of wide-ranging EU or national data protection laws.[213] Broadly speaking, individual data processing is essentially forbidden unless there is a valid reason for doing so and it is done as narrowly as possible.[214]

This EU recognition and protection of individual rights to data privacy is reflected in the NIS and ECI directives. Accordingly, the NIS Directive, in paragraph 75 to the preamble states:

> This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data. . . . This Directive should be implemented in accordance with those rights and principles.[215]

The ECI Directive contains a similar provision for critical infrastructure providers in general.[216] If a conflict arises, NIS and ECI directives need to be interpreted in light of the fundamental right to data privacy. This does not mean that a critical service provider or DSP would not be able to process personal data that is necessary to provide its life-critical service. Limitations are possible if provided for by law and the essence of the fundamental right is guaranteed.[217] With regard to critical infrastructure protection or network security, these legal grounds are provided for by the ECI or NIS directive. However, because data privacy is a fundamental right, limitations ought to be interpreted

---

Two Western Cultures of Privacy: Dignity Versus Liberty, 113 YALE L.J. 1151, 1173–76 (2004) (describing the evolution of privacy law in France).

211 ECFR art. 8(1), 2000 O.J. (C 364) 10; Consolidated Version of the Treaty on the Functioning of the European Union art. 16(1), Oct. 26, 2012, 2012 O.J. (C 326) 47. The ECFR is a compilation of all "personal, civic, political, economic and social rights enjoyed by people within the EU." *Why do we need the Charter?*, EUR. COMM'N, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en (last visited Nov. 1, 2020) [https://perma.cc/CTH5-WTTW]. It is different from the ECHR as it covers "all the rights found in the case law of the Court of Justice of the EU, the rights and freedoms enshrined in the European Convention on Human Rights, other rights and principles resulting from the common constitutional traditions of EU countries and other international instruments." *Id.*

212 So-called "third generation" fundamental right. *See* EUR. COMM'N, *supra* note 210. *See also* GDPR, *supra* note 160, pmbl., para. 1 (referencing ECFR, art. 8(1) and TFEU, art. 16(1) and stating, "[t]he protection of natural persons in relation to the processing of personal data is a fundamental right.").

213 *See* W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AM. BUS. L.J. 287, 290 (2019); *see also* Schwartz & Solove, *supra* note 160, at 880–881 (stating that "[i]n the European Union, privacy law is viewed in broad terms" and that "[g]iven these differences, it is no surprise that EU privacy law has a much broader definition of PII than U.S. privacy law.").

214 GDPR, *supra* note 160, art. 6, para. 1*; see also* Schwartz & Solove, *supra* note 160, at 881 ("[i]n the European Union, privacy law forbids personal data processing in the absence of a legal basis.").

215 NIS Directive, *supra* note 159, pmbl., para. 75.

216 ECI Directive, *supra* note 151, pmbl.

217 *See* ECFR, *supra* note 210, art. 52(1).

narrowly and the processing of personal data must be restricted to the "extent strictly necessary and proportionate."[218] This is different from the simple "balancing" between two rights under U.S. law.[219] Hence, in Europe, a mandatory cell phone app that helps the government track the spread of COVID-19 in the interest of public health is not illegal per se, but by design needs to be limited to process only personal data strictly necessary to fulfill its purpose.[220]

Building upon the criticality of a NoP infrastructure, the following section argues that the differing U.S. and EU approaches to critical infrastructure protection from threats and vulnerabilities is inadequate to protect it and should be standardized for a global approach to protecting fundamental rights and increasing national security.

C. Proposed Critical Protection for the NoP

From a U.S. perspective, an argument can be made that the CNoP should be categorized as a critical national infrastructure under its current structure. The DHS description of critical infrastructure poses the question of whether the system provides essential services that underpin American society and serve as the backbone of the nation's economy, security, and health. The disruptions described above, voting and patient safety, are certainly parts of our national backbone and deserving of critical protection. However, the United States is unlikely to view these as part of other infrastructures and will likely not recognize the citizen-centric harms that could arise. In large part, this is because of the United States's piecemeal approach to data privacy. Broadly, personally identifiable information is protected under certain federal privacy and state laws, rather than an integrated approach to protection, that leads to a narrow sectorial approach to data privacy.[221] The basic assumption in the United States is that private and government bodies are allowed to process individual data "unless it causes a legal harm or is otherwise restricted by law."[222] A detailed description of data privacy laws in both the United States and Europe is beyond the scope of this article, and has been expertly done elsewhere.[223] By means of

---

218 GDPR, *supra* note 160, pmbl., para. 49.

219 *See* Schwartz & Solove, *supra* note 160, at 880 (arguing that the constitutional right to privacy in the United States is a right of defense against governmental overreach). This explains why in the United States, an individual's expectation of privacy can be balanced against other interests.

220 Health data is treated as a special category of personal data and processing is only allowed under very narrow circumstances. GDPR, *supra* note 160, art. 9, para. 1; *see* GDPR, art. 9, para. 2.

221 *See* Schwartz & Solove, *supra* note 160, at 881 (stating in the United States sectorial laws "focus on specific industries or specific contexts for the use of personal data"); *see also* Voss & Houser, *supra* note 212, at 292 (arguing that distinguishing the terms "personal data" and "PII" is crucial to "understanding data privacy law as the terms delimit the scope of the law.").

222 Schwartz & Solove, *supra* note 160, at 6.

223 A small but growing body of scholarship addresses the differences between data privacy in the United States and the European Union, especially after the enactment of the EU GDPR and EU-U.S. Privacy Shield. S*ee* Voss & Houser, *supra* note 212, at 288 (citing Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. no. 1, at 44–52 (2018) (drawing lessons from a comparison of past U.S. and EU data privacy enforcement actions for enforcement of the GDPR); Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365 (2019), *https://ssrn.com/abstract=3239930* [https://perma.cc/94XL-L9BN] (arguing that there are "affinities" between U.S. and EU data privacy law and seeing transatlantic data privacy convergence on several points); Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1974–79 (2013) (commenting on transatlantic divergences after the proposal of the GDPR but before its enactment); Paul M. Schwartz & Karl-Niklaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 119–22 (2017) (taking the angle of "legal identities" on both

comparison, however, "[i]n the United States, privacy law focuses on redressing consumer harm and balancing privacy with efficient commercial transactions. In the European Union, privacy is hailed as a fundamental right that can trump other interests."[224]

In Europe, because privacy is considered an expression of a person's dignity, the NoP will more easily be recognized as a critical infrastructure. Human dignity, according to Article 1 of the EU Charter of Fundamental Rights of the European Union and national constitutions, is an inviolable fundamental right that deserves higher protection than any other right.[225] In the NoP, where the person becomes an integral part of the infrastructure, personal data is a natural extension of the person herself— and may thus qualify as a critical asset of the infrastructure. Given the NoP's reliance on personal data, a personal data breach is likely to pose a threat not only to the individual who owns or is concerned by that data, but indeed the entire infrastructure, hence justifying enhanced protection. Consider, for example, the impact a loss of confidence in the safety or confidentiality of personal data could have on voting, freedom of expression, union membership or other democratic rights, let alone the functioning of the digital economy. EU law recognizes these interdependencies. It is no coincidence that the NIS directive and GDPR were enacted in the same year. By European conception, cybersecurity and data protection are part of a cohesive digital strategy. It follows that critical infrastructure providers as well as DSPs who process personal data, are subject to both the notification requirements in the NIS directive and the GDPR.[226] Furthermore, as an example of national law, the German constitutional court as early as in 1983 addressed the relationship between personal data processing and individual liberties, summarized this way:

> According to the Court, individuals who do not know whether, which of, by whom, for what purposes, and under what conditions their personal data are processed will inevitably tend to conform themselves to the processor's potential expectations. In doing so, these individuals renounce their power to freely express their opinions, to demonstrate or join a political party, union, or any other association—in short, to exercise their fundamental rights. For this reason, the Court concluded that a democratic society cannot and will not function without rules governing the processing of personal data. [227]

Hence, it is no surprise that from a European perspective, data protection is seen as part of

---

sides of the Atlantic, in the context of transatlantic data trade). *See generally* Paul J. Watanabe, *An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure*, 90 S. CAL. L. REV. 1111 (2017) (making a comparison of privacy law related to the GDPR's right to erasure).

224 Schwartz & Solove, *supra* note 160, at 877.

225 *See* Carmen Moldovan, *Essential Features of the Principle of Human Dignity*, REVISTA UNIVERSUL JURIDIC 165, 165 (2016) (referencing the constitutions of Germany, Romania, and France as national constitutions that consider human dignity either "directly or implicitly as the top fundamental right in an hierarchy of fundamental freedoms"; *id.* at 166 (comparing human dignity's "non-derogatory nature" to other fundamental rights).

226 *See* JONES DAY, *supra* note 203, at 4 (noting that a data breach could trigger both, notification requirements under NIS and GDPR).

227 Spiros Simitis, *From the Market to the Polis: The Eu Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 447–48 (1995) (citing Volkszählungsurteil, 65 BVERFGE 43 (1983), *translated in* 5 HUM. RTS. L.J. 94 (1984)).

EU policy to achieve cyber resilience.[228] In this regard, EU critical infrastructure protection in the light of the general data protection regulation, may pave the way to a more seamless recognition of the concept of protection for the CNoP—centered around persons, and their data—as opposed to things. GDPR's impact has not been isolated to European citizens or markets. Laws such as GDPR are having an impact in the United States. The global nature of the Internet necessitates multinational legal and regulatory standards, and many U.S. firms are adhering to European law simply out of necessity.[229]

The fragmentation of American approaches to U.S. cybersecurity remains a challenge. Recent work done by the United States Cyberspace Solarium Commission reiterates many of the fundamental issues highlighted above.[230] The report provides strong support for the recognition of the impact of cybersecurity risks and vulnerabilities on individuals. Yet in its recommendations, the emphasis remains on governmental and public-private partnerships across sectors at levels above the individual.[231] By privileging higher-level actors, the impacted parties at lower levels are often consolidated by default into higher level organizational categorizations. Yet the concerns of individuals differ substantially from those of most public and private organizations. The objectives of the firm and the citizen are not the same. And the critical life functions of the latter are often not addressed by remediating cybersecurity concerns in the former.

Thus, a related but different question is whether personal data should be considered a unique part of the NoP, by itself, and consequently, enjoy the same infrastructure protection as security, public health, or network and information systems. As mentioned earlier, for purposes of defining a critical infrastructure that is entitled to protection by a partnership between government and private entities, the boundary is whether the NoP infrastructure affects critical life functions, deserving enhanced protection from threats and vulnerabilities.[232] If personal data is more broadly included, then data privacy would be added to the list of protected functions in Article 2(a) of the ECI directive, and the DHS definition of critical infrastructure, depending on whether data protection is considered "life critical," and its disruption or destruction would have a significant impact on society as a result of the failure to maintain its function.[233] Overcoming historical differences, a global adoption of this approach would yield heightened security around the globe.

IV. CONCLUSION

Intimately connected technology is increasingly interweaving persons in ways that extend the importance and relevance of critical infrastructure protections to the person. The present disjointed

---

228 AEGIS, *supra* note 146 (mentions the EU General Data Protection Regulation as well as the proposed e-Privacy Regulation on Privacy and Electronic Communications alongside the EU Directive on Security of Network and Information Systems (NIS Directive) as main EU measures to achieve cyber resilience).

229 *See* Flora Y. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, 33 HARV. J.L. & TECH. 661, 666–67) (2020) (discussing the arguments about whether the GDPR becomes a type of de jure regulation).

230 CYBERSPACE SOLARIUM COMMISSION, CSC, https://www.solarium.gov/home [https://perma.cc/Q2Z9-BPTY] (last visited Nov. 1, 2020).

231 CYBERSPACE SOLARIUM COMMISSION, *Report*, https://www.solarium.gov/report [https://perma.cc/PN3T-RF6N] (last visited Nov. 1, 2020).

232 *See* U.S. DEP'T OF TRANSP., *supra* note 62, at 14-16 (and accompanying text).

233 Adapted from ECI directive, art. 2 § (a).

and fragmented approaches of Europe and the United States exacerbate the problems and elevate the importance of reconsidering designations of critical infrastructure. A new designation of a CNoP does not obviate or alleviate the risks associated with the technologies; rather, it begins to shift the burden of risk mitigation and protection away from those least capable, towards the state and its partners. Just as individuals require the intervention of the state in times of severe insecurity due to natural or human induced disaster in conventional sectors, they similarly require the intervention of the state in the rapidly developing NoP infrastructure. The protection of life critical functions sustained and enhanced by the CNoP is concurrently a human rights and national security issue. The proposed CNoP framework integrates security from the individual outward, further impacting security at multiple levels.

Limiting critical infrastructures to higher levels within the digital ecosystem fails to address vulnerabilities associated with individuals embedded in the ecosystem, leaving open vulnerabilities and exposing populations to forces largely beyond their control. Proactively addressing the issue of CNoP begins the likely long and arduous process of ensuring security of citizenship, economic necessities, and personhood in an increasingly complex digital world. The risks posed by the NoP and to the infrastructure around it will grow in the coming years. A failure to address this concern will result in harms that are pervasive, systemic, and deleterious to the security of both the citizen and the nation.

Based on sensors, data collection and aggregation, internet communications, and decision triggers, this article establishes a foundation for understanding an infrastructure that both surrounds and integrates the individual as part of an inescapable structure: the NoP. The proposed CNoP framework defines life critical functions as fundamental rights and obligations in three areas: citizenship, economic necessities, and personhood. In an infrastructure connected by persons, these life-critical functions must become embedded into national security protection across all critical infrastructures. Ultimately, protecting the CNoP results in protecting the privacy and decisional integrity of individual data processing. The government, as the collective body of democratic deliberation within a society, formed for the protection of rights, is duty-bound to protect its citizenry. The U.S. Constitutional justification for the designation of the CNoP is enshrined in the obligation of common defense, general welfare, and security.[234] Securing the "Blessings of Liberty to ourselves and our posterity"[235] is at risk due to the pervasive and systemic challenges faced by citizenry as they increasingly become part of the structure to be secured. Establishing protection for the CNoP reorients the scope and focus to that of the citizen, the person—the building block of the nation. Ensuring the security at the individual level is imperative for maintaining national security for all.

234 U.S. CONST. pmbl.

235 *Id.*