

VOLUME 9

SPRING 2023

ISSUE 1

Journal of Law & Cyber Warfare

ARTICLES

- The Internet of Things (IoT) in a Post-Pandemic World.....1
Mohammed T. Hussein & Lawrence J. Trautman
- Deepfakes and the Law of Armed Conflict.....76
Summer Crockett

© 2024 by
Journal of Law & Cyber Warfare.
All Rights Reserved.

JOURNAL OF LAW & CYBER WARFARE

VOLUME 9

2023

ISSUE 1

Editor-in-Chief

DANIEL B. GARRIE
Partner, Law & Forensics LLP
Neutral, JAMS

Managing Editor

DOUGLAS SMITH

Staff Editors

JEREMY GORDON
JOSHUA PARSONS

Editorial Board

PARHAM EFTEKHARI

Co-Founder, ICIT

KEVIN FUMAI

Senior Managing Counsel,
Oracle Corp.

MALCOLM HARKINS

Chief Security and Trust Officer,
Cymatic

WILL HUDSON

Senior Advisor for Int'l
Policy, Google Inc.

ERIC JENSEN

Professor,
Brigham Young University

JOSEPH JOHNSON

CISO, Premise Health

DAVID LAWRENCE

Co-founder,
RANE Network

SHRADDHA PATIL

Director Product Management,
Palo Alto Networks

DR. JAMES RANSOME

Senior Director of Product
Security, McAfee

Conference Editor

SONYA MORGAN

Executive Editor

MICHAEL MANN

Business Editor

SARAH HAINES

Associate Business Editor

SOFIA MAHAIRAS

CHRISTOPHER BAILEY
AFAF FATIMA

RICHARD ANDRES

Professor,
National War College

ROBERT BARNSBY

Professor,
Army Cyber Institute

RICHARD BORDEN

Partner, Chief Privacy
Officer, White & Williams

DIANA BURLEY

Professor, George
Washington University

UMA CHANDRASHEKHAR

Information & Product
Safety Officer, Alcon

JAMES DEVER

Chief of Intelligence Law,
Army Intelligence

CHRIS DEMCHAK

Chair of Cyber Security,
US Naval War College,

MICHAEL DUFFY

Principal Consultant,
M2BD Associates

SALEELA SALAHUDDIN
LEONARD WONG

COL. SHANE REEVES

Professor, U.S. Military Academy
at West Point

MICHAEL SCHMITT
Professor,

Exeter University

MAJ. GEN. AMI SHAFRAN
Co-founder,
Wenspire

DAVID C. SHONKA

Partner
Redgrave LLP

RHEA SIERS

Cyber Defense Strategy
Executive, Bank of America

WILLIAM SPERNOW

Chief Forensic Advisor
Security Mentors, LLC

COL. DAVID WALLACE

Professor, U.S. Military Academy
at West Point

ELAD YORAN

CEO, Security
Growth Partners

The Internet of Things (IoT) in a Post-Pandemic World

Mohammed T. Hussein* & Lawrence J. Trautman**

ABSTRACT

Internet of Things (IoT) devices allow people to live smarter, safer and more productive lives, enabled in many cases by ‘smart systems’ in such key areas as health care, education, community ‘smart city’ living — and provide advances in productivity to help reduce global food insecurity and adverse developments brought about by climate change. The daily life of billions of individuals worldwide has been forever changed by IoT technology in just the last few years.

By 2024 the world remains mired in year four of dealing with a highly infectious pandemic; Russia is engaged in an invasion of Ukraine; war has erupted in the Middle-East; food insecurity is rapidly increasing; the World Bank and others warn of likely future economic distress; and adverse destructive weather events continue as the result of disruptive climate dynamics. Against this backdrop, Internet usage and penetration continues to grow, as does the number of devices connected to the Internet.

We proceed in thirteen sections. First, we set the stage for this discussion by focusing on humanity in crisis following the Covid-19 pandemic. Second, we define the Internet of Things (IoT), comment on the

* BS, Prairie View A&M University; M.S. Texas A&M University-Kingsville (electrical engineering); Ph. D., Texas A&M University (electrical engineering). Dr. Hussein is Assistant Professor of Management Information Systems (MIS) at Prairie View A&M University. He may be contacted at mthussein@pvamu.edu.

** BA, The American University; MBA, The George Washington University; J.D., Oklahoma City University School of Law. Mr. Trautman is Associate Professor of Business Law and Ethics at Prairie View A&M University; Associate Professor, Texas A&M University School of Law (by courtesy); External Affiliate, Indiana University Bloomington, Ostrom Workshops in Data Management & Information Governance, and Cybersecurity & Internet Governance. Professor Trautman is a past president of the New York and Washington, DC/Baltimore chapters of the National Association of Corporate Directors (NACD). He may be contacted at Lawrence.J.Trautman@gmail.com.

*** The authors wish to extend particular thanks to the following for their assistance in the research and preparation of this article: Subhi Alrubei; Beatriz Botero Arcila; Jody Blanke; Diana Bowman; Igor Calzada; Janine S. Hiller; Tania Kapiki; Kayleen Manwaring; Michele Molè; Mason J. Molesky; Lyria Bennett Moses; and Sarah Light. Thanks also to Gary Marchant and all those responsible for the 9th Annual Governance of Emerging Technologies and Science Conference, May 19-20, 2022, held at the Sandra Day O’Connor College of Law, Arizona State University. All errors and omissions are our own.

explosive growth in sensory devices connected to the Internet, provide examples of IoT devices, speak to the promise of the IoT; and discuss the IoT post-COVID-19. Third, we examine existing and potential IoT security threats. Fourth, is a discussion about the important role IoT plays in agriculture and assisting with the problem of global food insecurity. Fifth, we look at how IoT applications assisted during the COVID-19 pandemic. Sixth, climate change and environmental monitoring is discussed. Seventh, we look at IoT healthcare applications. Regulation is our Eighth topic. Ninth, the role of IoT and smart cities is explored. Tenth, is the significant role played by IoT applications and devices in the supply chain. Eleventh, we examine the topic of IoT and water. Worker safety is discussed next. And last, we conclude. We believe this Article contributes to understanding: our connected Internet; the widespread exposure to malware associated with IoT; and adds to the nascent but emerging literature on governance of enterprise and climate risk; all subjects of vital global societal importance.

CONTENTS

OVERVIEW	5
I. HUMANITY IN CRISIS	8
II. THE INTERNET OF THINGS (IoT).....	13
Growth of the Internet	13
Internet of Things (IoT).....	14
Explosive Growth of Connected Sensory Devices	18
Importance of Blockchain Technology	20
IoT Post Covid-19	22
III. POTENTIAL IoT SECURITY THREATS.....	24
Data Breaches and Ransomware Continue	24
Manufactured Usage Description (MUD) Methodology	28
Additional NIST Resources	29
IV. AGRICULTURE AND FOOD INSECURITY	31
Agricultural IoT Applications	32
Fishing Industry.....	34
V. COVID-19 PANDEMIC AND RELATED APPLICATIONS	36
Early Detection.....	36
Use of Drones.....	37
Population and Employee Monitoring	38
Technology Adoption Accelerates	40
VI. CLIMATE CHANGE AND ENVIRONMENTAL MONITORING	41
We Are All in This Together.....	41
Weather Induced Disaster Management	42
Corporate Sustainability Goals and IoT	43
The Age of Disinformation and Climate	43
The SEC and Environmental, Social & Governance Disclosure (ESG)	44
VII. HEALTHCARE	45
Medical Research	46
Telemedicine	48

	Diagnostic Facial Expressions	49
	Numerous IoT Healthcare Applications.....	49
VIII.	REGULATION	51
	Disclosure.....	51
	The SEC and Data.....	52
	The Corporate Governance Challenge	53
	Duty to Provide Data Security	54
	Leadership at the Top.....	56
	Board Talent, Experience, and Committees.....	57
	Recent Regulatory Update	57
IX.	SMART CITIES.....	58
	Smart Homes.....	62
X.	SUPPLY CHAINS	63
	NIST and Supply Chain Risk Management	65
	Supply Chains and Blockchain	69
XI.	WATER.....	70
	Flooding	72
XII.	WORKER SAFETY.....	73
	Sewage Environment Monitoring System.....	74
	Safety of Coal Miners	74
	Augmented Reality (AR) and Worker Safety	74
XIII.	CONCLUSION	75

The widespread incorporation of “smart” devices into everyday objects is changing how people and machines interact with each other and the world around them, often improving efficiency, convenience, and quality of life. Their deployment has also introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Cyber actors have already used IoT devices for distributed denial-of-service (DDoS) attacks, and we assess they will continue. In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks.

*Daniel R. Coats
Director of National Intelligence¹*

INTRODUCTION

By 2024 the world remains mired in its year four of dealing with a highly infectious pandemic;² Russia is engaged in an invasion of Ukraine;³ war has erupted in the Middle East;⁴ food insecurity is rapidly increasing;⁵ the World Bank and others warn of likely future economic distress;⁶ adverse destructive weather events continue as the result of disruptive climate

¹ *Worldwide Threat Assessment of the U.S. Intelligence Community, Before the S. Select Comm. on Intel.*, 115th Cong. 1 (2017) (statement of Daniel R. Coats, Director of National Intelligence).

² Julie Bosman, *Journey is Lonely for Those Who Lost Loved Ones*, N.Y. TIMES, May 15, 2022, at 32; *Covid Variants on the Rise*, WALL ST. J., June 8, 2022, at A1.

³ Ian Lovett, *Ukraine Strikes Back in East as It Awaits Stronger Rockets*, WALL ST. J., June 6, 2022, at A1. *See also* Matthew Mpoke Bigg & Maria Varenikova, *Zelensky Announces Criminal Inquiry into Attack at Soldier Ceremony*, N.Y. TIMES, Nov. 6, 2023, at A5.

⁴ Thomas Fuller, Aaron Boxerman, Malachy Browne & Neil Collier, *Gaza’s Hospitals Bear the Brunt as Battles Rage*, N.Y. TIMES, Nov. 11, 2023, at A1.

⁵ Mark Landler, Matina Stevis-Gridneff, Erika Solomon & Patricia Cohen, *As Food Remains Trapped in Ukraine, Leaders Warn of Global Unrest*, N.Y. TIMES, May 25, 2022, at A5.

⁶ Patricia Cohen, *World Bank Sees Economic Threat on Global Scale: Muted Growth Likely*, N.Y. TIMES, June 8, 2022, at A1; Andrew Duehren & Yuka Hayashi, *Yellen, World Bank Warn of Stubborn Inflation*, WALL ST. J., June 8, 2022, at A1; Patricia Cohen, *Latest Forecast Sees Continued Economic Pain*, N.Y. TIMES, June 9, 2022, at B4; Jeanna Smialek, *Prices Shoot Up Again, Squeezing Fed and Testing Biden’s Economic Policy: Increase Comes as a Surprise to Many Economists*, N.Y. TIMES, June 11, 2022, at A1; Michael S. Derby, *New York Fed Sees ‘Chances of a Hard Landing,’* WALL ST. J., June 18-19, 2022, at A2.

change;⁷ and Ukraine is now several years into defending itself from Russian invasion.⁸ Against this backdrop Internet usage and penetration continues to grow, as does the number of devices connected to the Internet. However, several experts interviewed by Pew Research believe that following four years of pandemic, things will be better for many because of technological “enhancements in virtual and augmented reality and AI that allow people to live smarter, safer and more productive lives, enabled in many cases by ‘smart systems’ in such key areas as health care, education and community living.”⁹

Today’s increasing rate of technological change results from the rapid growth in computer processing speed, particularly artificial intelligence applications, when combined with the cost decline of processing capacity, and is of historical import.¹⁰ Giaretta, Dragoni and Massacci report, “Smart homes are equipped with a growing number of IoT devices that capture more and more information about human beings’ lives. However, manufacturers paid little or no attention to security...”¹¹ As the U.S. National Institutes of Standards and Technology reports in their July 2019 exposure draft titled *Core Cybersecurity feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers*:

⁷ Christopher Flavelle, *Wildfire Risk to U.S. Homes Grows Greater*, N.Y. TIMES, May 17, 2022, at A1.

⁸ Lawrence J. Trautman & Maia McFarlin, *Putin, Russia and Ukraine: International Human Rights Violations, War Crimes, & Future Implications* (unpub. ms.), <http://ssrn.com/abstract=4393282>.

⁹ Janna Anderson, Lee Rainie & Emily A. Vogels, *Experts Say the ‘New Normal’ in 2025 Will Be Far More Tech-Driven, Presenting More Challenges*, PEW RESEARCH CENTER (Feb. 18, 2021), <https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges/>.

¹⁰ Scott Shackelford, Lawrence J. Trautman & W. Gregory Voss, *How We Learned to Stop Worrying and Love AI: Analyzing the Rapid Evolution of Generative Pre-Trained Transformer (GPT) and its Impacts on Law, Business, and Society*, 34 ALBANY L.J. SCI. & TECH. (forthcoming), <http://ssrn.com/abstract=4516154>. See also Michael J. Conklin, Brian Elzweig & Lawrence J. Trautman, *Legal Recourse for Victims of Blockchain and Cyber Breach Attacks*, 23(2) U.C. DAVIS BUS. L.J. 135 (2022-2023), <http://ssrn.com/abstract=4251666>; Mohammed T. Hussein, Munir Quddus & Lawrence J. Trautman, *The Impact of Technological Progression on Impoverished Countries*, (unpub. ms.), <http://ssrn.com/abstract=4504926>; Lawrence J. Trautman & Larry D. Foster II, *The FTX Crypto Debacle: Largest Fraud Since Madoff?*, 54 U. MEMPHIS L. REV. 289 (2023), <http://ssrn.com/abstract=4290093>; Lawrence J. Trautman, Scott Shackelford, Brian Elzweig & Peter C. Ormerod, *Understanding Cyber Risk: Unpacking and Responding to Cyber Threats Facing the Public and Private Sectors*, 78 U. MIAMI L. REV. 840 (2024), <https://ssrn.com/abstract=4262971>.

¹¹ See Alberto Giaretta, Nicola Dragoni & Fabio Massacci, *Protecting the Internet of Things with Security-by-Contract and Fog Computing*, in PROCEEDINGS OF 2019 IEEE 5TH WORLD FORUM ON INTERNET OF THINGS (WF-IOT) (2019).

Manufacturers are creating an incredible variety and volume of Internet of Things (IoT) devices, which incorporate at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface (e.g., Ethernet, WiFi, Bluetooth, Long-Term Evolution [LTE], ZigBee), and are not conventional IT devices for which the identification and implementation of cybersecurity features is already well understood (e.g., smartphone, laptop). Many IoT devices provide computing functionality, data storage, and network connectivity for equipment that previously lacked these functions. In turn, these functions enable new efficiencies and technological capabilities for the equipment, such as remote access for monitoring, configuration, and troubleshooting. IoT can also add the ability to analyze data about the physical world and use the results to better inform decision making, alter the physical environment, and anticipate future events.¹²

The daily life of billions of individuals worldwide has been forever changed by technology in just the last few years.¹³ Costly data breaches continue at an alarming rate.¹⁴ By 2020, “IoT devices were increasingly being implicated in cyber-attacks, raising community concern about the

¹² See MICHAEL FAGAN, KATERINA N. MEGAS, KAREN SCARFONE & MATTHEW SMITH, CORE CYBERSECURITY FEATURE BASELINE FOR SECURABLE IoT DEVICES: A STARTING POINT FOR IoT DEVICE MANUFACTURERS, DRAFT NISTIR 8259 (2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf>.

¹³ Some examples of these recent technological advances having profound impact include: Google (founded 1998), see Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-commerce, Political and Regulatory Compliance Risks*, 10 WM. & MARY BUS. L. REV. (2018), <https://ssrn.com/abstract=3067298> [https://perma.cc/23UM-L4Z4] (citing Alphabet Inc., Quarterly Report (Form 10-Q), at 17 (Oct. 27, 2017), PayPal, Registration Statement (Form S-1), at 9 (June 12, 2002), <https://www.sec.gov/Archives/edgar/data/1103415/000091205702023923/a2082068zs-1.htm> [https://perma.cc/7G9F-E8FL]; Lawrence J. Trautman, *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal*, 17 U.C. DAVIS BUS. L.J. 261, 274–79 (2016); Lawrence J. Trautman & Alvin Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?* 38 CARDOZO L. REV. 1041, 1055 (2017), <http://ssrn.com/abstract=2730983>; Uber (2009), see *Company Info*, UBER, <https://www.uber.com/newsroom/company-info/> [https://perma.cc/UDE2-9L54] (last visited Jan. 19, 2018); WhatsApp (2009), Parmy Olson, *Exclusive: The Rags-to-Riches Tale of how Jan Koum Built WhatsApp Into Facebook’s New \$19 Billion Baby*, FORBES (Feb. 19, 2014, 7:58 PM), <https://www.forbes.com/sites/parmyolson/2014/02/19/exclusive-inside-story-how-jan-koum-built-whatsapp-into-facebooks-new-19-billion-baby/> [https://perma.cc/ZRM5-22WM]; Instagram (2010); see Gwyn Topham, *Look Ma, Mo Hands: What will it Mean when all Cars can Drive Themselves?*, GUARDIAN (United Kingdom) (Nov. 25, 2017), <https://www.theguardian.com/business/2017/nov/25/autonomous-vehicles-when-all-cars-drive-themselves-what-will-it-mean> [https://perma.cc/8XRJ-3KNT].

¹⁴ See BRUCE MIDDLETON, A HISTORY OF CYBER SECURITY ATTACKS: 1980 TO PRESENT (Taylor & Francis, 2017); *infra* § III.

risks they pose to critical infrastructure, corporations, and citizens.”¹⁵ The international standards body, the Internet Engineering Task Force (IETF), in an effort to mitigate risk, “is pushing IoT vendors to develop formal specifications of the intended purpose of their IoT devices, in the form of a Manufacturer Usage Description (MUD), so that their network behavior in any operating environment can be locked down and verified rigorously.”¹⁶ The challenges facing humans as they attempt to govern the process of artificial intelligence, machine learning, and the impact of billions of sensory devices connected to the Internet is the subject of this Article.

We proceed in thirteen sections. First, we set the stage for this discussion by focusing on humanity in crisis following the Covid-19 pandemic. Second, we define the Internet of Things (IoT), comment on the explosive growth in sensory devices connected to the Internet, provide examples of IoT devices, speak to the promise of the IoT; and discuss the IoT post-COVID-19. Third, we examine existing and potential IoT security threats. Fourth, is a discussion about the important role IoT plays in agriculture and assisting with the problem of global food insecurity. Fifth, we look at how IoT applications assisted during the COVID-19 pandemic. Sixth, climate change and environmental monitoring is discussed. Seventh, we look at IoT healthcare applications. Regulation is our Eighth topic. Ninth, the role of IoT and smart cities is explored. Tenth, is the significant role played by IoT applications and devices in the supply chain. Eleventh, we examine the topic of IoT and water. Worker safety is discussed next. And last, we conclude. We believe this Article contributes to understanding: our connected Internet; the widespread exposure to malware associated with IoT; and adds to the nascent but emerging literature on governance of enterprise and climate risk; all subjects of vital global societal importance.

I. HUMANITY IN CRISIS

¹⁵ See Ayyoob Hamza, Dinesha Ranathunga, Hassan Habibi Gharakheili, Matthew Roughan & Vijay Sivaraman, *Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles*, IOT S&P '18 PROCEEDINGS OF THE 2018 WORKSHOP ON IOT SECURITY AND PRIVACY (2018); see also Sarah Coble, *Amazon Doorbell Camera Lets Hackers Access Household Network*, INFOSECURITY MAGAZINE (Nov. 7, 2019), <https://www.infosecurity-magazine.com/news/amazon-doorbell-camera/>; Angella Foster, Op-Ed, *When Parents Spy on Nannies*, N.Y. TIMES, Aug. 20, 2019, at A23; Sandra E. Garcia, *Maker of Popular Home Security Camera Exposes Users*, N.Y. TIMES, Dec. 31, 2019, at B4; Kate Murphy, *Is There a Tiny Spy in Your TV Room? How to Unmask It*, N.Y. TIMES, Nov. 16, 2019, at B1; Zack Whittaker, *Amazon Ring Doorbells Expose Home Wi-Fi Passwords to Hackers*, TECHCRUNCH (Nov. 7, 2019), <https://techcrunch.com/2019/11/07/amazon-ring-doorbells-wifi-hackers/>.

¹⁶ See Hamza, *supra* note 15.

So the Internet and the accompanying information revolution has been transformative. And there's no turning back. But like all advances in technology, this process has had unintended consequences that sometimes come at a price. And in this case, we see that our new information ecosystem is turbocharging some of humanity's worst impulses.

*Barack Obama
Stanford University
April 21, 2022¹⁷*

During November 2021, nation states representing approximately 75% of worldwide carbon emissions were attending the two-day G20 summit meeting held in Rome “struggled to find a consensus on how best to adhere to the 2015 Paris climate agreement.”¹⁸ Just days later, at the COP26 Glasgow climate summit, “Diplomats from nearly 200 countries... struck a major agreement aimed at intensifying global efforts to fight climate change... calling on governments to return next year with stronger plans to curb their planet-warming emissions and... ‘at least double’ funding to protect poor nations from the hazards of a hotter planet.”¹⁹ *The New York Times* warns:

The new deal will not, on its own, solve global warming, despite the urgent demands of many of the thousands of politicians, environmentalists and protesters who gathered at the Glasgow climate summit. Its success or failure will hinge on whether world leaders will follow through with new policies to cut greenhouse gas emissions. And the deal still leaves vulnerable countries far short of the funds they need to cope with increasing weather disasters.²⁰

In a fact sheet issued following the Glasgow summit, the U.S. White House observes, “On his first day in office, President Biden rejoined the Paris Agreement, restored U.S. leadership on the world stage, and

¹⁷ Barack Obama, Former U.S. President, Keynote address at Challenges to Democracy in the Digital Information Realm symposium, *Disinformation as a Threat to Our Democracy* (April 21, 2022), <https://barackobama.medium.com/my-remarks-on-disinformation-at-stanford-7d7af7ba28af>.

¹⁸ Max Colchester, Sha Hua & Matthew Dalton, *Limited Progress on Climate at G-20 Signals Hurdles Ahead*, WALL ST. J., Nov. 1, 2021, at A1.

¹⁹ Brad Plumer & Lisa Friedman, *Negotiators Strike a Climate Deal, but World Remains Far From Limiting Warming*, N.Y. TIMES (Nov. 13, 2021), <https://www.nytimes.com/2021/11/13/climate/cop26-glasgow-climate-agreement.html>.

²⁰ *Id.*

reestablished our position to tackle the climate crisis at home and abroad.”²¹ Among other steps taken, “Congress passed President Biden’s Bipartisan Infrastructure Deal, which will expand access to clean drinking water, make unprecedented investments in clean energy infrastructure, and is a critical step towards reaching our goal of a net-zero emissions economy by 2050.”²² Consider:

As the U.S. engaged in intensive diplomacy and partnership with countries around the world, collective action increased global ambition, innovation, and action to tackle the climate crisis. At the close of COP26:

- 90% of the world’s GDP now has net zero commitments and 154 countries put forward new climate action plans to cut emissions or “NDCs”. In April, President Biden announced a new target for the United States to achieve a 50-52 percent reduction from 2005 levels in economy-wide net greenhouse gas pollution in 2030 and convened the Leaders’ Summit on Climate to secure stronger targets from world leaders.
- The United States and European Union announced that over 100 countries, covering nearly half of global methane emissions and almost 70% of global GDP signed the Global Methane Pledge, including six of the world’s top 10 methane emitters. This complements the U.S. Methane Emissions Reduction Action Plan – bold steps announced by President Biden to redouble efforts from across the government to dramatically reduce U.S. methane emissions, cut consumer costs, protect workers and communities, maintain and create thousands of high-quality, union jobs, and promote U.S. innovation and manufacturing of critical new technologies.
- Developed countries made progress towards the \$100 billion climate finance mobilization goal. In April, President Biden has released the first-ever U.S. International Climate Finance Plan and announced a quadrupling of the U.S. international climate finance pledge at the UN General Assembly in September, including the largest U.S.

²¹ Press Release, White House, Fact Sheet: Renewed U.S. Leadership in Glasgow Raises Ambition to Tackle Climate Crisis, The White House (Nov. 13, 2021), <https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/13/fact-sheet-renewed-u-s-leadership-in-glasgow-raises-ambition-to-tackle-climate-crisis/>.

²² *Id.*

commitment ever made to reduce climate impacts on those most vulnerable to climate change worldwide.

- The U.S. announced our first-ever contribution to the Adaptation Fund which at COP26 received \$356 million in new support from contributing national and regional governments. President Biden announced the launch of the President's Emergency Plan for Adaptation and Resilience (PREPARE), a whole-of-government initiative that will serve as the cornerstone of the U.S. Government response to addressing the increasing impacts of the global climate crises in order to enhance global stability.
- Twenty-five countries, including the United States, and five financial institutions pledged to end new international finance for unabated fossil fuel energy by the end of 2022, except in limited and clearly defined circumstances that are consistent with the 1.5 degrees Celsius warming limit, reorienting tens of billions of dollars of public finance and trillions of private finance towards low carbon priorities.
- Over \$20 billion of new public and philanthropic finance has been committed to support developing countries to transition away from coal.
- Countries representing 90% of global forest cover pledged to reduce deforestation to zero by 2030, backed by the biggest ever commitment of public funds for forest conservation and a global roadmap to make 75% of forest commodity supply chains sustainable. Twelve countries signed the Global Forest Finance Pledge: a target of \$12 billion to combat deforestation. The United States released the Plan to Conserve Global Forests: Critical Carbon Sinks, a first-of-its-kind, whole-of-government effort to preserve global ecosystems which serve as vital carbon sinks.
- The United States launched the First Movers Coalition with more than 25 Founding Members including some of the largest companies in the world, across a wide range of industries, with hundreds of billions of dollars in purchasing power. The buyers' clubs assembled by this initiative will create early market demand for innovations across eight "need-to-abate" sectors—steel, trucking, shipping, aviation, aluminum, concrete, chemicals, and direct air capture—which represent more than one-third of the

world's carbon emissions today, and is expected to grow in the coming decades.

- China joined the United States, the world's two biggest economies and emitters, in committing in a new Joint Declaration to collaborate on increased ambition to keep 1.5 degrees Celsius warming within reach, and China for the first time committed to develop a plan to address methane emissions and accelerate its coal phase-down.

- The United States, UK, EU, France, and Germany announced a partnership with South Africa to chart a course from coal to clean energy through the creation of new jobs and opportunities for South African coal communities. This partnership will seek to prevent up to 1-1.5 gigatons of emissions over the next 20 years in support of South Africa's accelerated transition to a low emission, climate resilient economy, and aims to mobilize \$8.5 billion for the first phase of financing, through various mechanisms including grants, concessional loans, investments, risk sharing, and other instruments for private sector mobilization. This partnership comes as the United States continues to redouble efforts to invest in our nation's energy communities, including delivering the largest investment in American history to tackle legacy pollution while creating thousands of new good paying jobs as part of the President's Bipartisan Infrastructure Deal.

- The United States and the United Arab Emirates launched the Agricultural Innovation Mission alongside more than 30 countries and more than 45 non-government partners to increase and accelerate agricultural and food systems innovation in support of climate action. The initiative has already garnered an \$4 billion in increased investment in climate smart agriculture and food systems innovation, with the United States planning to mobilize \$1 billion over five years.²³

²³ *Id.*

II. THE INTERNET OF THINGS (IoT)

In the digital area, Our economies' future increasingly depends on people's ability to connect to secure information and communications technologies. And we need to strengthen the use of trusted technologies so that our online information cannot be used by autocrats to consolidate their power or repress their people.

*Joseph R. Biden
U.S. President
Remarks at Meeting of the G7
June 26, 2022²⁴*

The Internet of Things (IoT) can be defined as “a vast network of devices that are connected to the internet and, consequently, each other increasingly.”²⁵ In the simplest of terms, any sensory device that may find connectivity to the Internet is a part of the Internet of Things. Included are wearables such as: watches or any sensory devices that are worn on clothing to detect health vitals such as heart rate, body temperature, blood pressure; smart phones; and all those household devices such as front door video cameras, plant and gardening watering needs, voice command devices to control televisions, room temperature, etc. Military sensory applications are robust: IoT remote sensory devices monitor troop and vehicle movement; sonar and space sensory applications; vital signs of healthy and wounded troops in the battle theatre, just to name a few.²⁶

A. Growth of the Internet

²⁴ Joe Biden, President, Remarks by President Biden at Launch of the Partnership for Global Infrastructure and Investment (June 26, 2022), <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/06/26/remarks-by-president-biden-at-launch-of-the-partnership-for-global-infrastructure-and-investment/>.

²⁵ NIST, *Securing Small Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks by Using Manufactured Usage Description*, Nat'l Cybersecurity Center of Excellence (May 26, 2021), <https://www.nist.gov/publications/securing-small-business-and-home-internet-things-iot-devices-mitigating-network-based> (last viewed May 30, 2024).

²⁶ Sarah E. Light, *Valuing National Security: Climate Change, the Military, and Society*, 61 UCLA L. REV. 1772 (2014); Sarah E. Light, *The Military-Environmental Complex*, 55 B.C. L. REV. 879 (2014).

Exhibit 1 depicts world Internet usage and population statistics reflecting estimates as of 2023.

Exhibit 1

Global Internet Usage and Population Penetration Rate²⁷

WORLD INTERNET USAGE AND POPULATION STATISTICS 2023 Year Estimates						
World Regions	Population (2022 Est.)	Population % of World	Internet Users 31 Dec 2021	Penetration Rate (% Pop.)	Growth 2000-2023	Internet World %
Africa	1,394,588,547	17.6 %	601,940,784	43.2 %	13,233 %	11.2 %
Asia	4,352,169,960	54.9 %	2,916,890,209	67.0 %	2,452 %	54.2 %
Europe	837,472,045	10.6 %	747,214,734	89.2 %	611 %	13.9 %
Latin America / Carib.	664,099,841	8.4 %	534,526,057	80.5 %	2,858 %	9.9 %
North America	372,555,585	4.7 %	347,916,694	93.4 %	222 %	6.5 %
Middle East	268,302,801	3.4 %	206,760,743	77.1 %	6,194 %	3.8 %
Oceania / Australia	43,602,955	0.5 %	30,549,185	70.1 %	301 %	0.6 %
WORLD TOTAL	7,932,791,734	100.0 %	5,385,798,406	67.9 %	1,392 %	100.0 %
NOTES: (1) Internet Usage and World Population Statistics estimates are for June 30, 2022. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the United Nations Population Division . (4) Internet usage information comes from data published by Nielsen Online , by the International Telecommunications Union , by GfK , by local ICT Regulators and other reliable sources. (5) For definitions, navigation help and disclaimers, please refer to the Website Surfing Guide . (6) The information from this website may be cited, giving the due credit to www.internetworldstats.com . Copyright © 2022, Miniwatts Marketing Group. All rights reserved worldwide.						

Source: [www.internetworldstats.com](#).

Many in North America may be shocked to learn that while North America accounts for 4.7 percent of global population, this equates to only 6.5 percent of worldwide population of Internet users. For 2023, it appears that North America enjoys an over 93 percent penetration rate, growth for the period 2000-2023 was 222 percent. Contrast these statistics with the Asian experience: over 67 percent penetration rate; twenty-three-year growth rate of 2,452 percent; and population about twelve (12) times that of North America. With a twenty-year growth rate of an astonishing 13,233 percent, Africa has a current penetration rate approximating only 43.2 percent. In addition, the estimated population is almost four-times that of North America.

B. Internet of Things (IoT)

Within recent years many scholars have written about the Internet of Things (IoT).²⁸ For Example, Bruce Sinclair contends that, “the Internet of

²⁷ Internet Usage and World Population Statistics (last viewed Nov. 11, 2023), <https://www.internetworldstats.com/stats.htm>.

Things (IoT) is just an evolution of the Internet. No more, no less. But the business ramifications of IoT are revolutionary and will usher in the Outcome Economy.”²⁹ Mr. Sinclair focuses upon how “The Internet of Things killer app is outcomes. It’s outcomes that customers usually want. They don’t even care about products: they care about what products do for them.... Customers don’t want to own cars, they want to get from one place to another, fast and safe.”³⁰ Businesses and customers depend upon reliable IoT outcomes. For example, during June 2022, “Some U.S. Starbucks stores across several days struggled to fulfill mobile orders and credit-card transactions for stretches of time, as cafes contended with mobile-ordering and payment-processing disruptions.”³¹ *The Wall Street Journal* reports that “Online and to-go orders are a vital part of Starbuck’s business. Around 75% of Starbuck’s U.S. Company store sales were placed through mobile ordering, on a delivery app or at drive-through windows [recently].”³²

Accordingly, Trautman and Ormerod warn that “The proliferation of novel consumer devices and increased Internet-dependent business and government data systems introduces vulnerabilities of unprecedented magnitude.”³³ IoT-related “Digital vulnerabilities touch upon numerous legal issues: breach notification,³⁴ constitutional provisions,³⁵ corporate

²⁸ Bronwyn Fox, Gerard Coggin, Deborah Lupton, Holger Regenbrecht, Paul Scuffham & Branka Vucetic, *The Internet of Things*, AUSTRALIAN COUNCIL OF LEARNED ACADEMIES (2020) <https://acola.org/hs5-internet-of-things-australia/>; Sarah Turner & Leonie Tanczer, *In Principle Vs in Practice: User, Expert and Policymaker Attitudes Towards the Right to Data Portability in the Internet of Things*, 52 COMPUT. L. & SEC. REV. (2024), <https://ssrn.com/abstract=4486266>.

²⁹ BRUCE SINCLAIR, IOT INC.: HOW YOUR COMPANY CAN USE THE INTERNET OF THINGS TO WIN IN THE OUTCOME ECONOMY xi (McGraw Hill Education, 2017).

³⁰ *Id.* at xxii.

³¹ Heather Haddon, *Tech Glitches Slow Orders at Coffee Giant*, WALL ST. J., June 18, 2022, at B3.

³² *Id.*

³³ See Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761, 764 (2018), <http://ssrn.com/abstract=2982629>; (citing Trey Herr & Allan A. Friedman, *Redefining Cybersecurity*, 8 AMERICAN FOREIGN POLICY COUNCIL - DEFENSE TECHNOLOGY PROGRAM BRIEF (2015), <https://ssrn.com/abstract=2558265>; Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227 (2003), <https://ssrn.com/abstract=416740>).

³⁴ Neal F. Newman, Lawrence J. Trautman & Brian Elzweig, *The SEC Proposed Cybersecurity Infrastructure Rules and New Disclosure Requirements*, UMKC L. REV. (forthcoming), <https://ssrn.com/abstract=4536669>; Trautman & Ormerod, *supra* note 33, at 765 (citing Fabio Bisogni, *Evaluating Data Breach Notification Laws - What Do the Numbers Tell Us?*, TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy (Aug. 15, 2013) (unpub. ms.), <https://ssrn.com/abstract=2236144>; Dana Lesemann, *Once More Unto the Breach: An Analysis of Legal, Technological and Policy Issues Involving Data Breach Notification*

governance³⁶ (including the duties of care,³⁷ to monitor,³⁸ and disclosure³⁹), information and data security,⁴⁰ inter-device interaction;⁴¹ law of war,⁴² privacy,⁴³ risk management,⁴⁴ securities regulation,⁴⁵ and more.⁴⁶

Statutes, 4 AKRON INTELL. PROP. J. 203 (2010), <https://ssrn.com/abstract=1671082>; Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007), <https://ssrn.com/abstract=908709>; Jane K. Winn, *Are 'Better' Security Breach Notification Laws Possible?*, 24 BERK. TECH. L. J. 1133 (2009), <https://ssrn.com/abstract=1416222>.

³⁵ *Id.* (citing Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28 ALBANY L.J. SCI. & TECH. 73 (2018), <https://ssrn.com/abstract=3005714>).

³⁶ Trautman & Ormerod, *supra* note 33, at 764 (citing John Armour, Henry Hansmann & Reinier Kraakman, *Agency Problems, Legal Strategies, and Enforcement* (Oxford Legal Studies Research Paper No. 21/2009), <https://ssrn.com/abstract=1436555>; Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 29 J. MARSHALL J. COMPUTER & INFO. L. 313 (2011), <http://www.ssrn.com/abstract=1947283>).

³⁷ Trautman & Ormerod, *supra* note 33, at 773 (citing Stephen M. Bainbridge, Star Lopez & Benjamin Oklan, *The Convergence of Good Faith and Oversight* (UCLA School of Law, Law-Econ Research Paper No. 07-09, 2007), <https://ssrn.com/abstract=1006097>; Melvin A. Eisenberg, *The Duty of Good Faith in Corporate Law*, 31 DEL. J. CORP. L. 1 (2005), <https://ssrn.com/abstract=899212>).

³⁸ *Id.* (citing Robert T. Miller, *The Board's Duty to Monitor Risk After Citigroup*, 12 U. PA. J. BUS. L. 1153 (2010), <https://ssrn.com/abstract=1696166>).

³⁹ Trautman & Ormerod, *supra* note 33, at 765 (citing Bernard S. Black, *The Core Fiduciary Duties of Outside Directors*, ASIA BUS. L. REV. 3 (2001), <https://ssrn.com/abstract=270749>; Henry T. C. Hu, *Too Complex to Depict? Innovation, 'Pure Information,' and the SEC Disclosure Paradigm*, 90 TEX. L. REV. 1601 (2012), <https://ssrn.com/abstract=2083708>; Peter A. Swire, *Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Agencies*, 42 HOU. L. REV. 1333 (2006), <https://ssrn.com/abstract=842228>).

⁴⁰ Trautman & Ormerod, *supra* note 33, (citing Ian Brown, Lilian Edwards & Christopher Marsden, *Information Security and Cybercrime*, in *LAW AND THE INTERNET*, (L. Edwards, C. Waelde, eds., 3rd ed., 2009), <https://ssrn.com/abstract=1427776>; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010), <https://ssrn.com/abstract=1450006>; Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, in *SECURING PRIVACY IN THE INTERNET AGE*, (Radin & Chander, eds., 2008), <https://ssrn.com/abstract=583483>; Richard Warner & Robert H. Sloan, *Defending Our Data: The Need for Information We Do Not Have* (Aug. 1, 2016) (unpublished manuscript), <https://ssrn.com/abstract=2816010>; Josephine Wolff, *Models for Cybersecurity Incident Information Sharing and Reporting Policies*, TPRC 43: THE 43RD RESEARCH CONFERENCE ON COMMUNICATION, INFORMATION AND INTERNET POLICY PAPER (2014), <https://ssrn.com/abstract=2587398>).

⁴¹ Kayleen Manwaring & Roger Clarke, *Surfing the Third Wave of Computing: A Framework for Research into eObjects*, 31 COMP. L. & SEC. REV. 586 (2015); Kayleen Manwaring, *Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies*, 22 DEAKIN L. REV. 53 (2017); Kayleen Manwaring, *Emerging Information Technologies: Challenges for Consumers*, 17 OXFORD U. COMMONWEALTH L.J. 265 (2017); Kayleen Manwaring & Roger Clarke, *Is Your Television Spying on You?*

The Internet of Things Needs More Than Self-Regulation, AUSTRALIAN SOCIETY FOR COMPUTERS & LAW (Oct. 16, 2020).

⁴² See Steven M. Bellovin, Susan Landau & Herbert S. Lin, *Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications*, 3 J. CYBERSECURITY 59 (2017) <https://ssrn.com/abstract=2809463>; Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEORGETOWN J. INT'L L. 735 (2017), <https://ssrn.com/abstract=2932110>; Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense*, 38 STAN. J. INT'L L. 207 (2002), <https://ssrn.com/abstract=987046>; Dakota S. Rudesill, James Caverlee & Daniel Sui, *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box*, 3 SCIENCE AND TECHNOLOGY INNOVATION PROGRAM (2015), <https://ssrn.com/abstract=2676615>; Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare*, 50 TEX. INT'L L. J. 189 (2015), <https://ssrn.com/abstract=2481629>; Scott Shackelford, Scott Russell & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. (2016), <https://ssrn.com/abstract=2652446>; Christopher S. Yoo, *Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures*, in CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS (Jens David Ohlin, Kevin Govern, Claire Finkelstein, eds., 2015), <https://ssrn.com/abstract=2596634>.

⁴³ See Trautman & Ormerod, *supra* note 33, at 764, (citing Corey Ciocchetti, *The Privacy Matrix*, 12 U. FLA. J. TECH. L. & POL'Y, (2008), <https://ssrn.com/abstract=1090423>; Neil M. Richards & Jonathan H. King, *Big Data and the Future for Privacy*, in HANDBOOK OF RESEARCH ON DIGITAL TRANSFORMATIONS (Elgar ed., 2016), <https://ssrn.com/abstract=2512069>; Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061 (2009), <https://ssrn.com/abstract=1522605>; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV. 583 (2014), <https://ssrn.com/abstract=2312913>; Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357 (2006), <https://ssrn.com/abstract=699701>; Robert Kirk Walker, *The Right to be Forgotten*, 64 HASTINGS L. J. 257 (2012), <https://ssrn.com/abstract=2017967>).

⁴⁴ Trautman & Ormerod, *supra* note 33, at 764, (citing Liam M. D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J.L. & CYBER WARFARE 1 (2014), <https://ssrn.com/abstract=2424958>; Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance*, 43 LAW & SOCIAL INQUIRY 417 (2017), <https://ssrn.com/abstract=2974233>; Lawrence J. Trautman & Kara Altenbaumer-Price, *D&O Insurance: A Primer*, AM. U. BUS. L. REV. 337 (2012), <http://ssrn.com/abstract=1998080>).

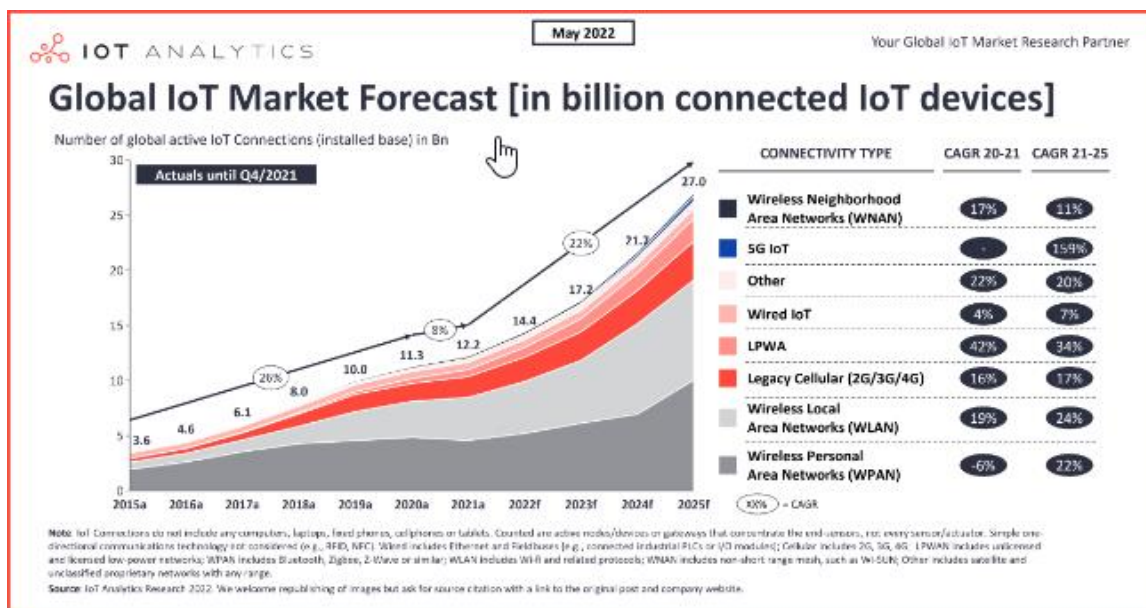
⁴⁵ Trautman & Ormerod, *supra* note 33, at 765, (citing Zohar Goshen & Gideon Parchomovsky, *The Essential Role of Securities Regulation*, 55 DUKE L.J. 711 (2006), <https://ssrn.com/abstract=600709>; Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security and Securities Regulation*, 3 BERKELEY BUS. L.J. 129 (2005), <https://ssrn.com/abstract=903263>; Robert B. Thompson & Hillary A. Sale, *Securities Fraud as Corporate Governance: Reflections Upon Federalism*, 56 VANDERBILT L. REV. 859 (2003), <https://ssrn.com/abstract=362860>; Lawrence J. Trautman & George P. Michaely, *The SEC & The Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L.Q. REP. 262 (2014), <http://www.ssrn.com/abstract=1951148>).

⁴⁶ See Trey Herr, Bruce Schneier & Christopher Morris, *Taking Stock: Estimating Vulnerability Rediscovery*, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS (2017), <https://ssrn.com/abstract=2928758>.

C. Explosive Growth of Connected Sensory Devices

IoT Analytics reports that because of global chip shortages “The number of global IoT connections grew by 8% in 2021 to 12.2 billion active endpoints, representing significantly lower growth than in previous years.”⁴⁷ In addition, “Despite a booming demand for IoT solutions... IoT Analytics expects the chip shortage’s impact... the number of connected IoT devices to last well beyond 2023... [with the 2022] market for the Internet of Things is expected to grow 18% to 14.4 billion active connections.”⁴⁸ Mid-2022 projections are “that by 2025, as supply constraints ease and growth further accelerates, there will be approximately 27 billion connected IoT devices.”⁴⁹ Exhibit 2 depicts the forecasted global IoT market forecast until 2025.

Exhibit 2
Global IoT Market Forecast⁵⁰



Source: IoT Analytics

During 2022, IoT Analytics forecasts the enterprise “IoT market size to grow at a CAGR of 22.0% to \$525 billion from 2022 until 2027. The

⁴⁷ Mohammed Hasen, *State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 billion Globally*, IoT ANALYTICS (May 18, 2022) (on file with authors).

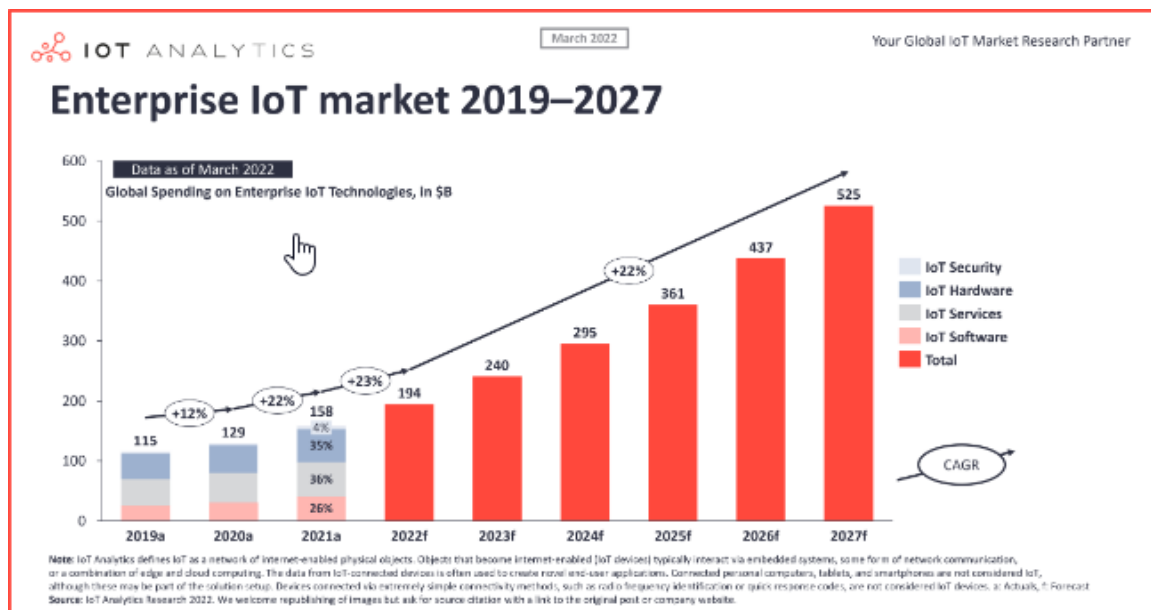
⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.*

five-year forecast has been lowered from the previous year.”⁵¹ Because “A number of growth headwinds have had a much more profound impact than previously anticipated, namely supply... and chip shortages... now expected to extend well into 2024 and... labor shortages, especially for sought-after software jobs.”⁵² Despite the lowered growth projections, IoT remains a very hot technology topic.”⁵³ Exhibit 3 illustrates the growth in Enterprise IoT revenues for the period 2019-2027.

Exhibit 3
Growth in Enterprise IoT Revenues, 2019-2027⁵⁴



Source: IoT Analytics

Exhibit 4 provides an example of just one of the many IoT devices that connect to the Internet. This example was found by conducting a

⁵¹ Philipp Wegner, *Global IoT Market Size Grew 22% in 2021 — These 16 Factors Affect the Growth Trajectory to 2027*, IoT ANALYTICS (Mar. 30, 2022) (on file with authors).

⁵² Mohammed T. Hussein, Lawrence J. Trautman & Reginald Holloway, *Technology Employment, Information and Communication in the Digital Age*, 103 J. U.S. PATENT & TRADEMARK OFF. SOC. 101 (2023), <https://ssrn.com/abstract=3762273>; Lawrence J. Trautman, *Rapid Technological Change and U.S. Entrepreneurial Risk in International Markets: Focus on Data Security, Information Privacy, Bribery and Corruption*, 49 CAP. U. L. REV. 67 (2021), <https://ssrn.com/abstract=2912072>.

⁵³ Wegner, *supra* note 51.

⁵⁴ *Id.*

Google Internet search. The thermostat was advertised for sale at \$17. While dozens of IoT sensors may be found in a typical smart home, “industrial applications can scale up to hundreds of IoT devices. This introduces several problems, such as maintaining and monitoring the IoT devices, allowing and disallowing communication protocols, and overseeing what kind of information can be shared under defined conditions.”⁵⁵

Exhibit 4
Example of Internet Connectivity Device⁵⁶



D. Importance of Blockchain Technology

In just a little over a decade blockchain technology has grown to be viewed with promise for its potential to provide enhanced software security.⁵⁷ Just a few of the other promising blockchain-enabled

⁵⁵ Lawrence J. Trautman, Mohammed T. Hussein, Louis Ngamassi & Mason Molesky, *Governance of the Internet of Things (IoT)*, 60 JURIMETRICS J. 315 (2020), <http://ssrn.com/abstract=3443973>.

⁵⁶ Google result from search for cheap Internet thermostat, (June 18, 2022), https://m.media-amazon.com/images/I/71Do18yKBmS._AC_SX679_.jpg.

⁵⁷ See Lawrence J. Trautman & Mason J. Molesky, *A Primer for Blockchain*, 88 UMKC L. REV. 239 (2019), <https://ssrn.com/abstract=3324660>.

applications include: autonomous agents;⁵⁸ autonomous vehicles;⁵⁹ cellular networks;⁶⁰ consensus mechanisms;⁶¹ non-fungible tokens;⁶² privacy;⁶³ security;⁶⁴ smart contracts;⁶⁵ virtual currencies;⁶⁶ and numerous financial services functions, including execution and clearing.⁶⁷ During 2018, Jianli Pan et al., write:

The emerging Internet of Things (IoT) is facing significant scalability and security challenges. On the one hand, IoT devices are 'weak' and need external assistance. Edge computing provides a promising direction addressing the deficiency of centralized cloud computing in scaling massive number of devices. On the other hand, IoT devices are also relatively 'vulnerable' facing malicious hackers due to resource constraints. The emerging

⁵⁸ Samuel Anbuselvan & Deepthi Nivasini Kumar, *The Impact of Innovative Technology and Autonomous Agents on Digital Transformation with Special Reference to Block Chain, (IoT) and AI*, 44 UGC CARE J. (2021), <https://ssrn.com/abstract=3890103>.

⁵⁹ Sankalp Chenna, *Blockchain and IoT as a Reinforcement for Vehicular Ad-hoc Network's (VANET's)* (Feb. 22, 2022), <https://ssrn.com/abstract=4041349>.

⁶⁰ Satya Ranjan Das, Santosh Kumar Behera & Gyana Ranjan Patra, *Internet of Things (IoT) and 5G Based Smart Algorithm*, 11 INT'L J. OF ADVANCED RES. IN ENG. & TECH. (IJARET) 183 (2020), <https://ssrn.com/abstract=3878692>.

⁶¹ Subhi Alrubei, Edward Ball & Jonathan Rigelsford, *HDPoA: Honesty-Based Distributed Proof of Authority Via Scalable Work Consensus Protocol for Iot-Blockchain Applications*, 217 COMPUTER NETWORKS (2022), <https://ssrn.com/abstract=3999127>.

⁶² Lawrence J. Trautman, *Virtual Art and Non-fungible Tokens*, 50 HOFSTRA L. REV. 361 (2022), <http://ssrn.com/abstract=3814087>; Brian Elzweig & Lawrence J. Trautman, *When Does a Nonfungible Token (NFT) Become a Security?*, 39 GA. ST. U. L. REV. 295 (2023), <http://ssrn.com/abstract=4055585>.

⁶³ Andy Crabtree, Hamed Haddadi & Richard Mortier, *Privacy by Design for the Internet of Things*, in *PRIVACY BY DESIGN FOR THE INTERNET OF THINGS: BUILDING ACCOUNTABILITY AND SECURITY* (Andy Crabtree, Hamed Haddadi & Richard Mortier eds., 2021), <https://ssrn.com/abstract=4002324>; Tanweer Alam, *A Survey On the Use of Blockchain for the Internet of Things*, 13 INT'L JOURNAL OF ELECTRONICS & INFO. ENGINEERING 119 (2021), <https://ssrn.com/abstract=3948064>.

⁶⁴ Shavan Askar, *Blockchain for Securing IoT Devices: A Review*, 5 INT'L JOURNAL OF SCIENCE AND BUSINESS (IJSAB) 209 (2021), <https://ssrn.com/abstract=3962701>.

⁶⁵ See Trautman & Molesky, *supra* note 57. See also Asma Khatoun & Nima Afraz, *Approaches to Adopt Blockchain Technology for Internet of Things* (Jan. 2, 2020), <https://ssrn.com/abstract=3930050>.

⁶⁶ See Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13 (2014), <http://ssrn.com/abstract=2393537>; Kinshuk Dua, *Implementation of an Efficient, Portable and Platform-Agnostic Cryptocurrency Mining Algorithm for Internet of Things Devices* (Feb. 14, 2022), <https://ssrn.com/abstract=4047844>.

⁶⁷ See Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 CONSUMER FIN. L.Q. REP. 232 (2016), <http://ssrn.com/abstract=2786186>.

blockchain and smart contracts technologies bring a series of new security features for IoT and edge computing.⁶⁸

One possible solution to these issues is an edge-IoT framework designed and prototyped called ‘EdgeChain.’ Jianli Pan et al., state “based on blockchain and smart contracts. The core idea is to integrate a permissioned blockchain and the internal currency or ‘coin’ system to link the edge cloud resource pool with each IoT device’ account and resource usage, and hence behavior of the IoT devices.”⁶⁹ Consider:

EdgeChain uses a credit-based resource management system to control how much resource IoT devices can obtain from edge servers, based on pre-defined rules on priority, application types and past behaviors. Smart contracts are used to enforce the rules and policies to regulate the IoT device behavior in a non-deniable and automated manner. All the IoT activities and transactions are recorded into blockchain for secure data logging and auditing. [Jianli Pan et al.] implement an EdgeChain prototype and conduct extensive experiments to evaluate the ideas. The results show that while gaining the security benefits of blockchain and smart contracts, the cost of integrating them into EdgeChain is within a reasonable and acceptable range.⁷⁰

Because blockchain applications appear useful to help solve many societal needs, we will provide comment and specific references throughout the remainder of our paper as appropriate.⁷¹

E. IoT Post Covid-19

As might be expected, application of the Internet to address potential solutions to many of the major problems facing humanity is now fully evident. During the heart of the U.S. pandemic crisis, by October 2021, IoT

⁶⁸ See Jianli Pan, Jianyu Wang, Austin Hester, Ismail Alqerm, Yuanni Liu & Ying Zhao, *EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts*, 6 IEEE INTERNET OF THINGS JOURNAL 4719 (2019).

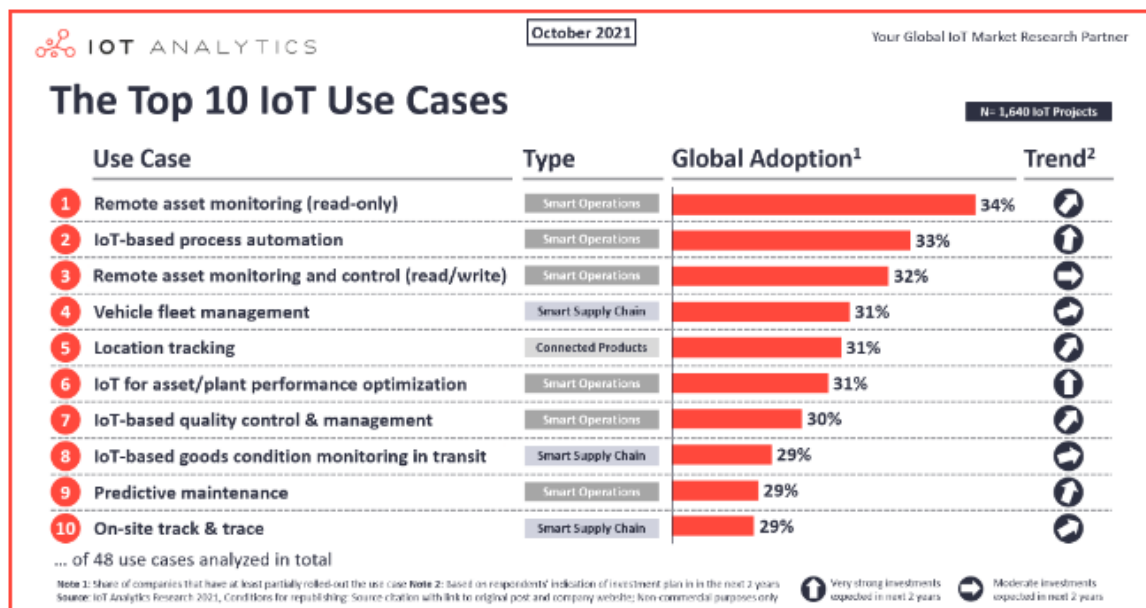
⁶⁹ *Id.*

⁷⁰ *Id.*; see also Subhi M. Alrubei, Edward Ball & Jonathan M. Rigelsford, *A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer*, 10 IEEE ACCESS (2022).

⁷¹ See *Infra* §§ IV, V, Vi, VII, VIII, IX, X, XI & XII; see also Kevin Werbach, *The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy*, 69 FLA. L. REV. 887 (2017); Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313 (2017), <https://ssrn.com/abstract=2936294>; Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321 (2007), <https://ssrn.com/abstract=932927>.

Analytics ranked by adoption the top 10 IoT use cases, observing that six of these “aim at making operations smart, thus improving companies’ production processes for manufacturing, enhancing, maintaining operations, or advancing any other operations (e.g., energy generation in the case of an energy company, running healthcare operations in the case of a hospital, or... store operations in... a retail company.”⁷² Exhibit 5 provides a listing of Top 10 IoT Use Cases as of that date.

Exhibit 5
Top 10 IoT Use Cases⁷³



Source: IOT Analytics

We will now look at potential security threats and how The Internet of Things (IoT) is viewed as a possible pathway for solutions to challenges from: agriculture; Covid-19 infections and preventative measures; climate change; healthcare; regulatory interface; smart cities; water management; and worker safety. The significant challenges from security risks associated with the growth of The Internet of Things will also be examined. Many of the issues we will now discuss are interrelated. For example, Professors Dasgupta and Robinson write “The links between climate change and food security are complex and many, and are well documented in the literature.

⁷² Philipp Wegner, *The Top 10 Use Cases*, IOT ANALYTICS (Oct. 13, 2021), <https://iot-analytics.com/top-10-iot-use-cases/>.

⁷³ *Id.*

The Intergovernmental Panel on Climate Change states with “high confidence” that climate change is already affecting food insecurity across the globe.”⁷⁴

III. POTENTIAL IoT SECURITY THREATS

[W]hile [cyber criminals] have become more sophisticated, governments have been sluggish in responding in a meaningful way. As a result, victims are often left to fend for themselves, turning to specialty incident response firms that have developed a niche industry for negotiating decryption. The costs of lost productivity, disrupted operations, inefficiency in markets, and operational recovery likely far outweigh the dollars siphoned out of the world’s economies and dumped into illicit activities from human trafficking to the development of weapons of mass destruction. That’s right - this malware has afforded Kim Jung Un’s ability to continue to expand his nuclear arsenal. How is this still only viewed as a cybercrime?

*Christopher C. Krebs
Congressional Testimony
May 5, 2021⁷⁵*

A. Data Breaches and Ransomware Continue

The following recital of significant data breaches are relevant to our discussion about IoT devices because any point of connectivity to the Internet is a potential threat vector. During May 2021, Colonial Pipeline, the U.S. “operator of a critical fuel pipeline on the East Coast paid extortionists roughly 75 Bitcoin — or nearly \$5 million — to recover its stolen data... after the cybercriminals [Darkside] ... held up the company’s

⁷⁴ Shouro Dasgupta & Elizabeth J.Z. Robinson, *Attributing Changes in Food Insecurity to a Changing Climate*, 12 SCIENTIFIC REPORTS (2022), <https://doi.org/10.1038/s41598-022-08696-x>. See also Mohammed T. Hussein, Munir Quddus & Lawrence K. Trautman, *The Impact of Technological Progression on Impoverished Countries* (July 9, 2023) (unpub. ms.), <http://ssrn.com/abstract=4504926>.

⁷⁵ *Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis: Hearings Before the H. Comm. on Homeland Security, Subcomm. on Cybersecurity, Infrastructure Protection, & Innovation*, 117th Cong. (2021) (statement by Christopher C. Krebs, Fmr. Dir. Of the Cybersecurity and Infrastructure Security Agency (CISA)).

business networks with ransomware... DarkSide is believed to operate from Eastern Europe, possibly Russia.”⁷⁶ *The New York Times* reported “The attacker... was a criminal extortion ring. The goal was not to disrupt the economy by taking a pipeline offline but to hold corporate data for ransom.”⁷⁷ The Colonial Pipeline attack produced “long lines of nervous motorists at gas stations — [which] stemmed not from a government response but from a decision by the victim... which controls nearly half the gasoline, jet fuel and diesel flowing along the East Coast, to turn off the spigot.”⁷⁸ Consider:

A confidential assessment prepared by the Energy and Homeland Security Departments found that the country could only afford another three to five days with the Colonial pipeline shut down before busses and other mass transit would have to limit operations because of a lack of diesel fuel. Chemical factories and refinery operations would also shut down because there would be no way to distribute what they produced, the report said.⁷⁹

Earlier major U.S. data breaches include: Target (December 2013);⁸⁰ Yahoo (2013, but not reported until several years later);⁸¹ Equifax (2017);⁸²

⁷⁶ Michael D. Shear, Nicole Perlroth & Clifford Krauss, *Colonial Pipeline Paid Roughly \$5 Million in Ransom to Hackers*, N.Y. TIMES (May 13, 2021),

<https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html>.

⁷⁷ David E. Sanger & Nicole Perlroth, *Pipeline Attack Yields Urgent Lesson About U.S. Cybersecurity*, N.Y. TIMES (May 14, 2021),

<https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html>.

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ See Maggie McGrath, *Target Data Breach Spilled Info on as Many as 70 Million Customers*, FORBES (Jan. 10, 2014),

<https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/>. See Rachel Abrams, *Target to Pay \$18.5 Million to 47 States in Security Breach Settlement*, N.Y. TIMES (May 23, 2017),

<https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html>.

⁸¹ See Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N. Y. TIMES (Sept. 22, 2016), <https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html>;

see also Robert McMillan, Ryan Knutson & Deepa Seetharaman, *Yahoo Discloses New Breach of 1 Billion User Accounts*, WALL ST. J. (Dec. 15, 2016),

<https://www.wsj.com/articles/yahoo-discloses-new-breach-of-1-billion-user-accounts-1481753131>;

Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231 (2017), <http://ssrn.com/abstract=2883607>.

⁸² See McKay Smith & Garrett Mulrain, *Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform*, 9 J. NAT'L SEC. L. & POL'Y 549 (2018); see also Scott J. Shackelford & Austin E. Brady, *Is It Time for A National Cybersecurity Safety Board? Examining the Policy Implications and Political Pushback*,

Office of Personnel Management (June 2015);⁸³ Marriott Hotels (January 2019);⁸⁴ and Capital One Financial Corp. (July 2019).⁸⁵ A more recent example is the hack of the world's largest bank, the New York unit of Industrial and Commercial Bank of China.⁸⁶ Many other examples exist, way too numerous to list here.⁸⁷

It appears that the billions of IoT sensors are the gateway for ransomware attacks.

Professors Trautman and Ormerod have previously provided an extensive account of the history and evolution of ransomware,⁸⁸ and we will not duplicate that effort here. The Federal Bureau of Investigation (FBI) defines ransomware as:

A type of malware installed on a computer or server that encrypts the files, making them inaccessible until a specified ransom is paid. Ransomware is typically installed when a user clicks on a malicious link, opens a file in an e-mail that installs the malware,

28 ALB. L.J. SCI. & TECH. 56 (2018); see also Spencer Kimball & Liz Moyer, *Equifax Data Breach May Affect 2.5 Million More Consumers than Originally Stated*, CNBC (Oct. 2, 2017), <https://www.cnn.com/2017/10/02/equifax-2-point-5-million-more-consumers-may-be-affected-by-data-breach-than-originally-stated.html>.

⁸³ *What Happened*, CYBERSECURITY RESOURCE CENTER: CYBER INCIDENTS, OPM, <https://www.opm.gov/cybersecurity-resource-center/>.

⁸⁴ Taylor Telford & Craig Timberg, *Marriott Discloses Massive Data Breach Affecting Up to 500 Million Guests*, WASH. POST (Nov. 30, 2018), <https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/>.

⁸⁵ See Stacy Cowley & Nicole Perlroth, *One Gap in Bank's Armor, and a Hacker Slips In*, N.Y. TIMES, July 31, 2019, at A1; Nicole Hong, Liz Hoffman & Anna Maria Andriotis, *Capital One Breach Affects 106 Million Card Applicants*, WALL ST. J., July 30, 2019, at A1; see also Robert McMillan, *Accused Hacker Exploited Vulnerability in Cloud*, WALL ST. J., Aug. 5, 2019, at A1; see also Dana Mattioli, Robert McMillan & Sebastian Herrera, *Hacking Suspect Left Trail of Clues Online*, WALL ST. J., July 31, 2019, at A1.

⁸⁶ Eric Wallerstein, Rebecca Feng & David Uberti, *Hack of Bank Poses New Test for Treasurers*, WALL ST. J., Nov. 11, 2023, at A1.

⁸⁷ Lawrence J. Trautman, Mohammed T. Hussein, Emmanuel U. Opara, Mason J. Molesky & Shahedur Rahman, *Posted: No Phishing*, 8 EMORY CORP. GOV. & ACCT. REV. 39 (2021), <http://ssrn.com/abstract=3549992>; Lawrence J. Trautman, *How Law Operates in a Wired Global Society: Cyber and E-Commerce Risk*, PROCEEDS OF THE KOREA LEGISLATION RESEARCH INSTITUTE (KLRI) 2017 LEGAL SCHOLAR ROUNDTABLE (Sept. 28, 2017), <https://ssrn.com/abstract=3033776>; Lawrence J. Trautman, *Managing Cyberthreat*, 33 SANTA CLARA HIGH TECH. L.J. 230 (2016), <http://ssrn.com/abstract=2534119>; Lawrence J. Trautman, Jason Triche & James C. Wetherbe *Corporate Information Technology Governance Under Fire*, 8 J. STRAT. & INT'L STUD. 105 (2013), <http://ssrn.com/abstract=2314119>.

⁸⁸ See Trautman & Ormerod, *supra* note 33.

or through drive-by downloads (which does not require user-installation) from a compromised Web site.⁸⁹

As just one example of a recently reported exploited IoT device, during 2021 *Forbes* reports that “A security researcher has found a show-stopping vulnerability in Hikvision surveillance cameras. Unpatched units are susceptible to remote hijacking, and the attacker doesn’t need a username or password to break in... Hikvision owns approximately 40% of the global surveillance camera market.”⁹⁰ On June 22, 2022 the *MIT Technology Review* writes that “Established in 2001, Hikvision started by selling video capture cards that are used in surveillance systems, but introduced its own video cameras in 2007. Today, it sells everything from software to hardware, usually at prices much cheaper than international competitors.”⁹¹ In 2008 Hikvision officially became “a subsidiary of a [Chinese] state-owned firm... [and] became an important part of China’s Skynet and Sharp Eyes policing projects, which aim to put cameras on every street to monitor citizens.”⁹² Fast-forward to 2021 and research discloses “4.8 million networks of Hikvision devices in 191 countries outside China. With over 600,000 Hikvision networks, the United States has the second-highest number of the Company’s cameras, just after Vietnam.”⁹³

According to the FBI, “hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.”⁹⁴ The U.S. Department of Homeland Security’s National Cybersecurity and Communications Integration Center (NCCIC)

⁸⁹ See *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*, Public Service Announcement, Alert No. I-091516-PSA, FED. BUREAU OF INVESTIGATION, <https://www.ic3.gov/Media/Y2016/PSA160915>.

⁹⁰ Lee Mathews, *Widely-Used Hikvision Security Cameras Vulnerable to Remote Hijacking*, *FORBES* (Sept. 22, 2021), <https://www.forbes.com/sites/leemathews/2021/09/22/widely-used-hikvision-security-cameras-vulnerable-to-remote-hijacking/>.

⁹¹ Zeyi Yang, *The World’s Biggest Surveillance Company You’ve Never Heard of*, *MIT TECHNOLOGY REVIEW* (June 22, 2022), <https://www.technologyreview.com/2022/06/22/1054586/hikvision-worlds-biggest-surveillance-company/>.

⁹² *Id.*

⁹³ *Id.* See also Lawrence J. Trautman, *Tik Tok! TikTok: Escalating Tension Between U.S. Privacy Rights and National Security Vulnerabilities* (Feb. 12, 2023) (unpub. ms.), <http://ssrn.com/abstract=4163203>.

⁹⁴ See *Cyber Crime: Key Priorities, Ransomware*, FBI (on file with authors). See also Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations*, 86 *TENN. L. REV.* 503 (2019), <http://ssrn.com/abstract=3238293>.

warns, “Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including: temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization’s reputation.”⁹⁵

During June 2016, Akamai reports starting to track a strain of malware that targets Internet of Things (IoT) devices and home Internet routers.⁹⁶ Soon thereafter, Mirai malware, spread worldwide.⁹⁷ Journalist Elie Bursztein considers the Mirai attack particularly remarkable because “they were carried out via small, innocuous Internet-of-Things (IoT) devices like home routers, air-quality monitors, and personal surveillance cameras. At its peak, Mirai infected over 600,000 vulnerable IoT devices.”⁹⁸ Cyber expert Brian Krebs released a story during December 2016 warning that:

New research published this week could provide plenty of fresh fodder for Mirai, a malware strain that enslaves poorly-secured Internet of Things (IoT) devices for use in powerful online attacks. Researchers in Austria have unearthed a pair of backdoor accounts in more than 80 different IP camera models made by Sony Corp. Separately, Israeli security experts have discovered trivially exploitable weaknesses in nearly a half-million white-labeled IP camera models that are not currently sought out by Mirai.⁹⁹

B. *Manufactured Usage Description (MUD) Methodology*

According to NIST, “Unfortunately, IoT devices often lack efficient and effective features for customers to use to help mitigate cybersecurity risks.”¹⁰⁰ The NIST internal report 8259 warns:

Consequently, some IoT devices are less easily secured using customers’ existing methods because the cybersecurity features

⁹⁵ See *Indicators Associated with WannaCry Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (June 7, 2018), <https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware>.

⁹⁶ See *Akamai’s State of the Internet Security: Q3 2016 Report*, AKAMI TECHNOLOGIES, INC. (2016), (on file with authors).

⁹⁷ *Id.*

⁹⁸ See Elie Bursztein, *Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis*, CLOUDFLARE: THE CLOUDFLARE BLOG (Dec. 14, 2017), <https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/>.

⁹⁹ Brian Krebs, *Researchers Find Fresh Fodder for IoT Attack Cannons*, KREBS ON SECURITY (Dec. 6, 2016), <https://krebsonsecurity.com/2016/12/researchers-find-fresh-fodder-for-iot-attack-cannons/>

¹⁰⁰ See Fagan, et al., *supra* note 12, at vii.

they expect may not be available on IoT devices or may function differently than is expected based on conventional IT devices. This means IoT device customers may have to select, implement, and manage additional or new cybersecurity controls or alter the controls they already have. However, new or tailored controls to sufficiently mitigate risks to the same level as before may not be available to all customers or implementable with all IoT devices. Compounding this problem, customers may not know they need to alter their existing IT processes to accommodate IoT. The result is many IoT devices are not secured properly, so attackers can more easily compromise them and use them to harm device customers and conduct additional nefarious acts (e.g., distributed denial of service [DDoS] attacks) against other organizations.¹⁰¹

A lack of standardization across the IoT marketplace led to a series of cyber-attacks and interoperability issues, resulting in development of the Manufactured Usage Description (MUD) as the industry's initial solution.¹⁰² The international standards body, Internet Engineering Task Force (IETF), moved the draft MUD standard into a quasi-accepted proposed standard RFC 8520 in March 2019.¹⁰³ In response to the release to RFC 8520, the National Institute of Standards and Technology (NIST) released a draft of NIST Special Publication (NIST SP) 1800-15: Securing Small-Business and Home Internet of Things (IoT) Devices – Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD).¹⁰⁴

C. Additional NIST Resources

As the U.S. Government's standards-setting body – particularly for cybersecurity standards – NIST is a rich resource for cybersecurity knowledge and materials.¹⁰⁵ NIST writes “Our work considers different device types, architectures, and configurations, and it tries to take a technology-agnostic approach whenever possible... we have consistently

¹⁰¹ *Id.*

¹⁰² Ryan McCauley, *The Internet of Things Needs Standardization – Here's Why*, GOVERNMENT TECHNOLOGY (Mar. 1, 2017), <https://www.govtech.com/fs/The-Internet-of-Things-Needs-Standardization-Heres-Why.html>.

¹⁰³ E. Lear, R. Droms & D. Romascanu, RFC 8520, *Manufacturer Usage Description Specification*, INTERNET ENGINEERING TASK FORCE (IETF) (Mar. 2019), <https://tools.ietf.org/html/rfc8520>.

¹⁰⁴ DONNA DODSON ET AL., NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBL'N NO. 1800-15A, SECURING SMALL BUSINESS AND HOME INTERNET OF THINGS (IoT) DEVICES: MITIGATING NETWORK-BASED ATTACKS USING MANUFACTURER USAGE DESCRIPTION (MUD) (Prelim. Draft Nov. 2019), <https://csrc.nist.gov/publications/detail/sp/1800-15/draft>.

¹⁰⁵ Federal Information Security Modernization Act of 2014, S. 2521, 113th Cong. (2014).

heard about cybersecurity challenges for both manufacturers and customers for particular types of IoT devices and systems, especially those that have constrained hardware.”¹⁰⁶ These constraints include such items as limited connectivity, limited energy supply, limited processing power or memory---combining to render objectives either difficult or impossible.¹⁰⁷ According to NIST:

Devices with constraints may often, but not always, face different, possibly lower risk than other equipment. NIST heard that these challenges are compounded when IoT systems are assembled from many constrained devices (e.g., a distributed sensor network), possibly creating a larger scale break of expectations about the cybersecurity capabilities of the system and its components. Additionally, IoT devices and systems of constrained or highly distributed architectures may face challenges implementing common technical (e.g., cybersecurity state awareness) and non-technical (e.g., documentation) cybersecurity measures. NISTIR 8228 considers some of these aspects, but stakeholders may benefit from more specific considerations based on what NIST has learned.¹⁰⁸

NIST continues to provide a constant stream of informative programs about IoT developments along with significant publications such as the Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products,¹⁰⁹ and the Report for the assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software: A summary review of labelling actions called for by Executive Order (EO) 14028: Improving the Nation’s Cybersecurity.¹¹⁰ We are including a few other sources here.¹¹¹

¹⁰⁶ Michael Fagan, *Cybersecurity for IoT: The Road We’ve Traveled, The Road Ahead*, NIST: CYBERSECURITY INSIGHTS (May 16, 2022), <https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-iot-road-weve-traveled-road-ahead>.

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

¹⁰⁹ NAT’L INST. OF STANDARDS & TECH., CYBERSECURITY WHITE PAPER 24, RECOMMENDED CRITERIA FOR CYBERSECURITY LABELING FOR CONSUMER INTERNET OF THINGS (IoT) PRODUCTS (Feb. 4, 2022), <https://csrc.nist.gov/publications/detail/white-paper/2022/02/04/criteria-for-cybersecurity-labeling-for-consumer-iot-products/final>.

¹¹⁰ *Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software: A summary review of labelling actions called for by Executive Order (EO) 14028: Improving the Nation’s Cybersecurity*, NAT’L INST. OF STANDARDS & TECH. (May 10, 2022), <https://www.nist.gov/system/files/documents/2022/05/24/Cybersecurity%20Labeling%20f>

IV. AGRICULTURE AND FOOD INSECURITY

Our analysis indicates that 74 developing countries, with a total population of 1.2 billion people, are particularly vulnerable to spiking food, energy and fertilizer costs.

António Guterres
Secretary General, United Nations
April 5, 2022¹¹²

By mid-2022, *The New York Times* writes that “The war in Ukraine has disrupted flows of food, fuel and minerals, adding to pandemic-related shortages and pushing inflation to multidecade highs.”¹¹³ At about the same time numerous reports of famine emerge, including warnings from the United Nations “that 18 million people in Africa’s Sahel region face severe hunger in the next three months, citing the impacts of Russia’s war in Ukraine, the coronavirus pandemic, climate-induced shocks and rising costs.”¹¹⁴ Professors Dasgupta and Robinson write “most of the literature

[or%20Consumers%20under%20Executive%20Order%2014028%20on%20Improving%20the%20Nation%27s%20Cybersecurity%20Report%20%28FINAL%29.pdf](https://ssrn.com/abstract=3853716).

¹¹¹ Irina Brass & Jesse Sowell, *Adaptive Governance for the Internet of Things: Coping with Emerging Security Risks*, 15 REGULATION & GOVERNANCE 1092 (2020), <https://ssrn.com/abstract=3853716>; Kashmira Ganji & Nikhat Afshan, *A Bibliometric Review of Internet of Things (Iot) on Cybersecurity Issues*, JOURNAL OF SCIENCE AND TECHNOLOGY POLICY MANAGEMENT (forthcoming 2024) <https://ssrn.com/abstract=4062860>; Giammaria Giordano, Fabio Palomba & Filomena Ferrucci, *Smart Detection and Preservation of Privacy Concerns in IoT Systems: A Systematic Literature Review* (unpub. ms.) (Dec. 7, 2021), <https://ssrn.com/abstract=3979390>; Joshua Streiff, Naheem Noah & Sanchari Das, *A Call for a New Privacy & Security Regime for IoT Smart Toys*, in PROCEEDINGS OF THE 2022 IEEE CONFERENCE ON DEPENDABLE AND SECURE COMPUTING (IEEE DSC 2022), <https://ssrn.com/abstract=4084004>; Otily Toutsop, Sanchari Das & Kevin Kornegay, *Exploring The Security Issues in Home-Based IoT Devices Through Denial of Service Attacks*, IEEE SMARTWORLD (SMARTWORLD/SCALCOM/UIC/ATC/IOP/SCI) 407 (2021), <https://ssrn.com/abstract=3897894>; Nanda Wagh & Sanjay Sutar, *A Smart Security Solution for Women's and Children Using Wearable IoT Systems* (unpub. ms.) (Jan. 3, 2022), <https://ssrn.com/abstract=3999107>.

¹¹² António Guterres, U.N. Secretary-General, Secretary-General’s Remarks at the UN Security Council Meeting on Ukraine (April 5, 2022), <https://www.un.org/sg/en/content/sg/speeches/2022-04-05/remarks-the-un-security-council-meeting-ukraine>.

¹¹³ Michael D. Shear & Ana Swanson, *Visiting Port of Los Angeles, Biden Casts Inflation as a Global Problem*, N.Y. TIMES, June 11, 2022, at A14.

¹¹⁴ Associated Press, *U.N. Says Millions Face Hunger in Sahel*, WALL ST. J., May 21-22, 2022, at A9.

addressing climate change impacts focuses on crop yields, production, and productivity, and future impacts of climate change, with much less attention given to the negative impact on food security that is already occurring.”¹¹⁵ The more recent outbreak of war in Gaza has only added to this problem.¹¹⁶

A. Agricultural IoT Applications

IoT technology enables “sensors [to] play an important role in modern agriculture. The use of sensors in various agriculture sectors minimizes the environmental impact on crops, helps in increasing yield and saving cost of operation.”¹¹⁷ The literature abounds with numerous IoT applications for agriculture. For example, Professors Bökle, Paraforos, Reiser and Griepentrog write, “Digitization in agriculture is rapidly advancing... New technologies and solutions were developed and get invented which ease farmers’ daily life, help them... to gain knowledge about farming processes and environmental interrelations. This knowledge leads to better decisions and contributes to increased farm productivity, resource efficiency, and environmental health.”¹¹⁸ Bökle et al. write how “Kim categorizes the applications of IoT fourfold in management systems, monitoring systems, control systems, and unmanned machinery, which include respectively a perception layer where physical properties are recognized, the network layer realizing M2M communication, and the application layer where the data is being used or processed to information.”¹¹⁹ In addition, “Chaudhary conducted a case study on AGCO’s Fuse Technology’s ‘Connected Farm Services’ as a commercial IoT example covering farm management, standard field works, monitoring, and dealer telemetries. They mention as major vulnerability issues the centrally connected network and the therefore comprehensive need of cyber security measures.”¹²⁰ IoT systems may help farmers to determine the best

¹¹⁵ Shouro Dasgupta & Elizabeth J.Z. Robinson, *Attributing Changes in Food Insecurity to a Changing Climate*, 12 SCI REP. 4709 (2022), <https://doi.org/10.1038/s41598-022-08696-x>.

¹¹⁶ Helene Cooper, Eric Schmitt & Adam Goldman, *U.S. Sees Danger in War Dragging On*, N.Y. TIMES, NOV. 10, 2023, at A1.

¹¹⁷ Arjuna Marzuki & Soh Yan Ying, *Environmental Monitoring and Controlling System for Mushroom Farm with Online Interface*, 9 INT’L J. COMPUTER SCI. & INFO. TECH. (IJCSIT) (2017), <https://ssrn.com/abstract=3898986>.

¹¹⁸ Sebastian Bökle, Dimitrios S. Paraforos, David Reiser & Hans W. Griepentrog, *Conceptual Framework of a Decentral Digital Farming System for Resilient and Safe Data Management*, 2 SMART AGRICULTURAL TECH. (2022), <https://ssrn.com/abstract=3995105>.

¹¹⁹ *Id.* (citing W.-S. Kim, W.-S. Lee, Y.-J. Kim, *A Review of the Applications of the Internet of Things (IoT) for Agricultural Automation*, 45 J. BIOSYST. ENG. 385-400 (2020), <https://doi.org/10.1007/s42853-020-00078-3>).

¹²⁰ Bökle *supra* note 118.

crops to grow given particular soil, climate, temperature, etc.¹²¹ Other authors when discussing IoT applications describe how “an automated process is applied to reduce the amount of water wastage by utilizing [a] smart irrigation pump feature... assist farmers with yield rate and planting process... decision making about harvest time... data storage, visualization, and management.”¹²²

Professors Vallakati, Ghosh, Thakur and Rathod write, “Smart farming helps us to... manage our farm effectively... not only push[ing] our yield further... but also focuses on optimum preservation of resources. Using means of modern technology... drastically reduces the farmer’s workload... teach[ing] the skill of adapting to climate changes.”¹²³ Smart farming using AI and IoT offer the following objectives:

- To increase the accuracy and efficiency of agricultural input applications;
- To ensure high crop productivity;
- Minimize the use of pesticides, fertilizers, and water;
- Reduce the strain on environment
- Low disposal of chemicals into groundwater and rivers.; and
- To deliver this technology to a wide segment of local researchers, environmentalists, farmers and agro-economists.¹²⁴

Others have illustrated the use of IoT for hydroponic farming to tailor differing plant requirements for pH values and properly maintain levels of pH, humidity, water level, temperature, and light intensity with the

¹²¹ Bhushan Jadhav, Rishabh Kriplani, Rahul Badugu & Ritesh Keswani, *Intelligent Farming Using IoT & Machine Learning*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SMART DATA INTELLIGENCE (ICSMDI 2021) (May 25, 2021), <https://ssrn.com/abstract=3852982>.

¹²² MD. Bayazid Rahman, Joy Dhon Chakma, A.S.M. Shafi, Shaheena Sultana & Wahidur Rahman, *Intelligent Crop Transplanting, Harvesting Prediction and Management Through Real Time Agricultural Monitoring System in the Context of Bangladesh: Smart Farming Environment Using Iot* (unpub. ms.) (Feb. 12, 2022), <https://ssrn.com/abstract=4001352>.

¹²³ Nagraj Vallakati, Tomal Ghosh, Shatayu Thakur & Mansing Rathod, *Smart Farming Using AI and IoT*, in PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON ADVANCES IN SCIENCE & TECHNOLOGY (ICAST2021) (May 7, 2021), <https://ssrn.com/abstract=3866432>.

¹²⁴ *Id.*; see also Arushi Agarwal, Manish Singh, Satyam Singh, Anand Singh & Atil Singh, *Wireless Sensor Network Based Internet of Things for Precision Agriculture*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INNOVATIVE COMPUTING & COMMUNICATION (ICICC) (Feb. 10, 2022), <https://ssrn.com/abstract=4031983>.

use of sensors.¹²⁵ Mechanical engineering hydroponic farming provides advantages of automated watering and fertilization and reduced labor by eliminating the need for soil preparation.”¹²⁶ Elsewhere, Professors Harkare and Neole present a solution for detection of swarming locusts utilizing image processing and ultrasonic sensors.¹²⁷

B. Fishing Industry

Former U.S. ambassadors to the World Trade Organization Peter Allgeier and Michael Punke, write “Fisheries can be a renewable source of food and jobs, but only if they are harvested in a sustainable manner.”¹²⁸ Ambassadors Allgeier and Punke warn, “The United Nations’ Food and Agriculture Organization estimates that 34 percent of the world’s ocean fish stocks, constituting almost a quarter of the seafood produced, are already fished to the point of being biologically unsustainable.”¹²⁹ Consider:

An additional 60 percent are currently fully fished — they can’t afford a further increase in fishing. Recognizing this, some leaders from the seafood retail sector are increasingly calling for an end to harmful fisheries subsidies, to ensure the longevity of their supply chains and to respond to consumer demand for fish that is sustainably, responsibly and legally caught.

The global fish trade generated \$164 billion in revenue in 2018 and accounted for nearly 40 percent of the world’s caught or farmed fish. In the United States, the commercial fishing industry employs 1.2 million people.¹³⁰

There can be little doubt that fishing and fish farming is an important source of nutrition for much of the world. Professors Shinde, More, Paithane, Rane and Phadke observe that, “Fish farming is one of the

¹²⁵ S. Gokul, Ismail Mulla, Nagaraja K, Pramoth Sakthi & Revathi GP, *Smart Hydroponic System Using IOT*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INNOVATIVE COMPUTING & COMMUNICATION (ICICC) (July 12, 2021), <https://ssrn.com/abstract=3884824>.

¹²⁶ *Id.*

¹²⁷ Ankita H. Harkare & Bhumi A. Neole, *A System for Detection of Locusts Swarms in Farms Using IoT*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SMART DATA INTELLIGENCE (ICSMDI 2021) (May 24, 2021), <https://ssrn.com/abstract=3852029>.

¹²⁸ Peter Allgeier & Michael Punke, Op-Ed, *The World Can’t Keep Fishing Like This*, N.Y. TIMES, June 14, 2022, at A23.

¹²⁹ *Id.*

¹³⁰ *Id.*

main occupations in rural areas of India.”¹³¹ IoT sensors are useful for measuring “water characteristics such as temperature, water level, ph... all displayed on a web page.”¹³² Elsewhere, professor Karim Aboul-Dahab describes the use of IoT for seafood product tracing by “using electronic product code technologies and Serial Shipping Container Code (SSCC) as a unique identifier to trace the fish crates along the supply chain process... [suggests] that IoT technology can improve quality management capability, logistics management competence, and competitiveness of domestic and international trade in... seafood traceability.”¹³³ Professor Aboul-Dahab:

proposed an IOT that monitor water quality using four different sensors that measures temperature, dissolved oxygen, potential hydrogen (pH) value and water level, the data was calculated in a specific time span and then transferred to the central processor. The central processor processes the parameters received and if the parameters are exceeding the threshold values it gives the buzzer signal and then corresponding relay is activated to bring back the measured value to the normal level, moreover the system send the measured value back to the authorized person for review via email and short message.¹³⁴

The world remains mired in over four years of dealing with the highly infectious Covid-19 pandemic.¹³⁵ We will now examine some of the ways in which IoT applications have played an important role in mitigating corona virus infections.

¹³¹ Swati Shinde, Saurabh More, Prafull Paithane & Shivam Rane, *IOT Based Fish Farming and its Applications*, in PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON ADVANCES IN SCIENCE & TECHNOLOGY (ICAST2021) (May 7, 2021), <https://ssrn.com/abstract=3866419>.

¹³² *Id.*

¹³³ Karim Aboul-Dahab, *The Role of Vessel Monitoring Systems (Vms) in Mitigating Illegal, Unreported and Unregulated (Iuu) Fishing*, THE INTERNATIONAL MARITIME TRANSPORT AND LOGISTICS CONFERENCE (MARLOG 10) (April 12, 2022), <https://ssrn.com/abstract=4081953>, (citing N. Vedachalam, M. Ravindran, & M. A. Atmanand, *Technology Developments for the Strategic Indian Blue Economy*, 37 MARINE GEORESOURCES & GEOTECHNOLOGY, 828-844, <https://doi.org/10.1080/1064119x.2018.1501625>).

¹³⁴ *Id.*; (citing Sérgio A. Mulema & Andrés C. García, *Monitoring of an Aquatic Environment in Aquaculture Using a MEWMA Chart*, 504 AQUACULTURE 275 (Apr. 15, 2019), <https://doi.org/10.1016/j.aquaculture.2019.01.019>).

¹³⁵ Julie Bosman, *Journey Is Lonely for Those Who Lost Loved Ones*, N.Y. TIMES, May 15, 2022, at 32; *Covid Variants on the Rise*, WALL ST. J., June 8, 2022, at A1; Joyu Wang & Rebecca Feng, *Covid Cases Rattle Markets in China*, WALL ST. J., July 12, 2022, at A18; Eddie Bernice Johnson & Lawrence J. Trautman, *The Demographics of Death: An Early Look at Covid-19, Cultural and Racial Bias in America*, 48 HASTINGS CONST. L.Q. 357 (2021), <http://ssrn.com/abstract=3677607>.

V. COVID-19 PANDEMIC AND RELATED APPLICATIONS

Today, the Centers for Disease Control and Prevention (CDC) is announcing a new center designed to advance the use of forecasting and outbreak analytics in public health decision making... [To] accelerate access to and use of data for public health decision-makers who need information to mitigate the effects of disease threats, such as social and economic disruption. We are excited to have the expertise and ability to model and forecast public health concerns and share information in real-time to activate governmental, private sector, and public actions in anticipation of threats both domestically and abroad.

*Rochelle P. Walensky, M.D.,
M.P.H.
Director, Centers for Disease
Control and Prevention (CDC)
August 18, 2021¹³⁶*

A. Early Detection

Professors Mondal, Ghosh, Gupta and Basu write that during the first year of the pandemic, “Most efforts to find a cure or control the spread of Covid-19 have not produced adequate results, and there is a great need for comprehensive monitoring of patients affected with Covid-19 infection.”¹³⁷ However, “during the Covid-19 pandemic, IoT technology has proven to be of great value in helping patients, healthcare providers, and government agencies.”¹³⁸ As is the case with many public health emergencies, it “is essential to diagnose Covid-19 sooner in order to prevent

¹³⁶ Press Release, Centers for Disease Control and Prevention, CDC Stands Up New Disease Forecasting Center (Aug. 18, 2021), <https://www.cdc.gov/media/releases/2021/p0818-disease-forecasting-center.html>.

¹³⁷ Sanjoy Mondal, Indrakshi Ghosh, Sayak Ghosh, Ayushi Gupta & Dipankar Basu, *Role of the Internet of Things for Early Detection of Covid-19 Infections: a Comprehensive Survey*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON IoT BASED CONTROL NETWORKS & INTELLIGENT SYSTEMS (ICICNIS) (July 8, 2021), <https://ssrn.com/abstract=3882424>.

¹³⁸ *Id.*; see also Beatriz Botero Arcila, *A Human Centric Framework to Evaluate the Risks Raised by Contact-Tracing Applications*, ICT4PEACE (Apr. 22, 2020), <https://ssrn.com/abstract=3653502>.

disease from spreading globally.”¹³⁹ By 2021, “Almost 190+ countries are taking necessary precautions and... virus spread is threatening the citizens of the affected countries... medical departments and government officials... are protecting their citizens by keep the infected persons in either quarantine centers or at their home or isolation based on the disease spread level.”¹⁴⁰ At that time:

Officials are fighting hard to contain the spread before it reaches pandemic level. The role of internet of medical things (e.g. current electronic health records Blood Pressure meters, Temperature readings, heart rate, pulse readings, blood sugar level meters) will do remote monitoring for impacted patients who are away from medical center and deep learning technologies like image detection or classification of x-ray or scanned body images to match the covid-19 image and predict the patients’ current spread level and organ impact. The collection of data from IOMT (Internet of Medical Things) will be kept in cloud storage for building the machine learning or deep learning models to predict the patient’s health risk. The blockchain plays a vital role on securing the IOMT devices and protect the citizen’s privacy information intact.¹⁴¹

B. Use of Drones

An emerging technology known as The Internet of Drone Things (IoDT) “has attracted significant attention in both academic and industry. IoDT is a technology that combines the Internet of Things, cloud/edge computing, wireless communication, and so on... It can perform critical missions (e.g., monitoring underground coal mines) with higher accuracy than humans.”¹⁴² In some parts of the world the pandemic has resulted in

¹³⁹ Sanjoy Mondal, Indrakshi Ghosh, Sayak Ghosh, Ayushi Gupta & Dipankar Basu, *Role of the Internet of Things for Early Detection of Covid-19 Infections: A Comprehensive Survey*, PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON IoT BASED CONTROL NETWORKS & INTELLIGENT SYSTEMS (ICICNIS) (July 8, 2021), <https://ssrn.com/abstract=3882424>.

¹⁴⁰ R. Chinnaiyan & S. Balachandar, *Connected Healthcare Framework for Remote Monitoring of Home Quarantined and Discharged COVID-19 Patients Using Internet of Medical Things (IOMT)* (May 27, 2021) (unpub. ms.) (on file with The Lancet), <https://ssrn.com/abstract=3854649>.

¹⁴¹ *Id.*; see also Alan Butler & Enid Zhou, *Disease and Data in Society: How the Pandemic Expanded Data Collection and Surveillance Systems*, 70 AM. U. L. REV. 1577 (2021), <https://ssrn.com/abstract=3836914>.

¹⁴² Anik Islam, Tariq Rahim, MD Masuduzzaman & Soo Young Shin, *A Blockchain-Based Artificial Intelligence-Empowered Contagious Pandemic Situation Supervision Scheme Using Internet of Drone Things*, IEEE WIRELESS COMMUNICATIONS (2021).

IoT usage of drones or “Unmanned Aerial Vehicles (UAVs) “for fumigation and sanitizing the places where the potential virus spread in different physical locations of the city, the combination of IOMT, Drones, and Artificial Intelligence and cloud platform will ... help the medical practitioners to predict the patients’ health.”¹⁴³ The use of drones may also assist city officials to “create a buffer zone to contain the spread through social distancing and restricted public movements on the impacted buffer zones.”¹⁴⁴

C. Population and Employee Monitoring

Other scholars have shown how “Artificial Intelligence (AI) has now become a required part of the medical sector, especially with the development of integrated circuits, sensors, and cameras... the spread of COVID-19 around the world and other spreadable diseases made the countries call for a complete lockdown for all sectors of life.”¹⁴⁵ In some countries such as India, as the COVID-19 situation during 2021 was “getting worse and death rates... increasing... wearing [a] mask has become a necessity for each individual.”¹⁴⁶ Writing during 2021, Professors Fulzele, Kirad, Dubey, Kulkarni and Thatte write that because of COVID-19, “Face mask detection has become a necessity... [and accordingly propose] utilizing cloud capabilities for face recognition.”¹⁴⁷ Elsewhere, medical doctors Manote and Matinun Arpornsuwan also acknowledge that “Early diagnosis of... COVID-19 is crucial for disease treatment and control.”¹⁴⁸ However, during 2020, at that time “none of [the] COVID-19 research mentioned that facial flushing was a clinical feature that could be found. The invisible facial flushing, unrecognized clinical sign with the naked eye

¹⁴³ Chinnaiyan & Balachandar, *supra* note 140.

¹⁴⁴ *Id.*

¹⁴⁵ Omar Mowaffak Alsaydia, Noor Raad Saadallah, Fahad Layth Malallah & Maan A. S. AL-Adwany, *Limiting COVID-19 Infection by Automatic Remote Face Mask Monitoring and Detection Using Deep Learning with IoT*, 5 EASTERN-EUROPEAN JOURNAL OF ENTERPRISE TECHNOLOGIES no. 2 (113) 29–36 (2021), doi:10.15587/1729-4061.2021.238359, <https://ssrn.com/abstract=3957564>; Antonio Aloisi & Valerio De Stafano, *Essential Jobs, Remote Work and Digital Surveillance: Addressing the Covid-19 Pandemic Panopticon*, 161 INT’L LABOUR REV. 289 (2022).

¹⁴⁶ Vaidehi Fulzele, Purva Kirad, Chanchal Dubey, Yash Kulkarni & Surabhi Thatte, *Utilizing Cloud Capabilities for Face Detection and Face Recognition During COVID-19: Comparative Analysis*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SMART DATA INTELLIGENCE (ICSMDI) (May 25, 2021), <https://ssrn.com/abstract=3853004>.

¹⁴⁷ *Id.*

¹⁴⁸ Manote Arpornsuwan, & Matinun Arpornsuwan, *Facial flushing in COVID-19: Subclinical Characteristic Unrecognized and Invisible to the Naked Eye*, 12 INT’L J. CURRENT RES. 10445-10446 (May 2020), <https://ssrn.com/abstract=3639037>.

could be detected by the smartphone application in the COVID-19 patients.”¹⁴⁹

Michele Molè writes that “The COVID-19 pandemic unveiled a new centrality of workplace surveillance. In particular, Artificial Intelligence (AI) and the Internet of Things (IoT) gained an important role as employee supervisors, with the outlook of remaining so in the post-pandemic scenario.”¹⁵⁰ In addition, “Although AI and IoT surveillance have made it possible to manage critical phases in workplaces (e.g. monitoring workers at home, checking body temperature and physical distancing), they also opened up unprecedented surveillance opportunities.”¹⁵¹ Consider:

Recording any activity performed on devices and generating inferences to predict employee behaviours have been normalised in employment routines. Indeed, AI devices are often complemented with IoT networks (such as laptops, smartphones and smart wristbands) to collect data and information about the working environment, whether virtual or physical, and the workforce.

Employers do have various legitimate surveillance needs, including protecting assets, managing risk, ensuring employee productivity and safeguarding against legal liability. Yet the necessary and proportionate implementation of surveillance through AI and IoT is often questioned. As highlighted by Eurofound (2020), they usher in a new wave of surveillance able to reveal more information than intended and/or necessary to meet employer needs. As a matter of fact, the AI and IoT revolution is portrayed as bringing about a ‘genetic variation’ in the distribution of power and information in employment. In other words, a structural overexposure of the workforce to employer scrutiny.

A recurring question thus runs through the scholarship and jurisprudence. Does this new surveillance respect privacy and

¹⁴⁹ *Id.*

¹⁵⁰ Michele Molè, *The Quest for Effective Fundamental Labour Rights in the European Post-Pandemic Scenario: Introducing Principles of Explainability and Understanding for Surveillance Through AI Algorithms and IoT Devices*, in 19TH INTERNATIONAL CONFERENCE IN COMMEMORATION OF MARCO BIAGI "WORK BEYOND THE PANDEMIC. TOWARDS A HUMAN-CENTRED RECOVERY" (May 1, 2022), <https://ssrn.com/abstract=4099663>, citing Manuela Samek Lodovici, *The Impact of Teleworking and Digital Work on Workers and Society. Special Focus on Surveillance and Monitoring, as Well as on Mental Health of Workers*, Policy Department for Economic, Scientific and Quality of Life Policies Directorate General for Internal Policies (Brussels: European Parliament, 2021), [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662904/IPOL_STU\(2021\)6629_04_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662904/IPOL_STU(2021)6629_04_EN.pdf).

¹⁵¹ *Id.*

fundamental labour rights? The answer is frequently negative across the literature: power and information asymmetries reveal shortcomings in transparency, fairness and accountability of AI and IoT as employer supervising means.¹⁵²

D. Technology Adoption Accelerates

The stresses of global pandemic resulted in severe global changes in human behavior and workplace dynamics. Almost overnight, entire populations were subjected to quarantine, resulting in immediate travel restrictions, empty restaurants and resort destinations. Millions of persons in the knowledge industry transitioned to working from home. As a result, mobile communications exploded and new work platforms such as Zoom received widespread adoption. As Zoom disclosed, “Beginning in the fiscal quarter ended April 30, 2020, we faced unprecedented usage of our communications platform largely due to the COVID-19 pandemic... we expect our user growth rate to continue to slow or decline as the impact of... COVID-19... continues to taper.”¹⁵³ Abhijit Mazumder, CIO of Tata Consultancy Services states “Across almost all sectors, the Covid-19 crisis has not only reduced the span of digital strategy from a couple of years to months but also made digital and corporate strategies one and the same and more imperative than ever before.”¹⁵⁴ We will now turn our attention toward the impact of IoT on climate and environmental issues.

¹⁵² *Id.*; see also Evan Selinger & Woodrow Hartzog, *The Inconsistency of Facial Surveillance*, 66 LOYOLA L. REV. 101 (2019), <https://ssrn.com/abstract=3557508>; Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1 (2020), <https://ssrn.com/abstract=3769613>.

¹⁵³ Zoom Video Communications, Inc., Annual Report (Form 10-K) 4 (March 18, 2022), <https://www.sec.gov/ix?doc=/Archives/edgar/data/1585521/000158552122000037/zm-20220131.htm>.

¹⁵⁴ Abhijit Mazumder, *Rapid Adoption of Emerging Technologies in the Wake of the Pandemic Requires Long-Term Thinking*, FORBES (Feb. 4, 2022), <https://www.forbes.com/sites/forbestechcouncil/2022/02/04/rapid-adoption-of-emerging-technologies-in-the-wake-of-the-pandemic-requires-long-term-thinking/>; see also David Leslie, *Tackling COVID-19 Through Responsible AI Innovation: Five Steps in the Right Direction*, HARV. DATA SCI. REV. (SPECIAL ISSUE 1) (2020), <https://ssrn.com/abstract=3652970>.

VI. CLIMATE CHANGE AND ENVIRONMENTAL MONITORING

Like other Small Island developing States, the Republic of Seychelles recognizes that building resilience to climate change and committing to a low-emission development pathway provide a firm basis for continued growth and sustainable development. We view climate change as an increasingly dire emergency that challenges all aspects of our chances for future survival and undermines Seychelles' effort to fully achieve the sustainable development goals.

Wavel John Charles Ramkalawan
President, Republic of the Seychelles
November 1, 2021¹⁵⁵

A. We Are All in This Together

Climate, like the Covid-19 global pandemic, illustrates how the population of the Earth is dependent on mutual cooperation for the survival of the planet. Professors Trautman and Newman have observed,¹⁵⁶ “It has been almost six decades since Rachel Carson’s ominous warning of pending environmental disaster.¹⁵⁷ During 2019 the United Nations requested urgent action from world leaders, given that at that time “just over a decade is all that remain[ed] to stop irreversible damage from climate change.”¹⁵⁸ With every passing year, damage resulting from destructive climate change causes increased pain, suffering, death and massive property loss.”¹⁵⁹ The

¹⁵⁵ National Statement by Mr. Wavel John Charles Ramkalawan President of the Republic of Seychelles on the Occasion of COP26/CMP16/CMA3.0 - World Leaders' Summit (WLS), High-Level Segment, 1-2 November 2021 Glasgow, UK (Nov. 2, 2021), https://unfccc.int/sites/default/files/resource/SEYCHELLES_cop26cmp16cma3_HLS_EN.pdf.

¹⁵⁶ Lawrence J. Trautman & Neal F. Newman, *The Environmental, Social and Governance (ESG) Debate Emerges from the Soil of Climate Denial*, 53 U. MEMPHIS L. REV. 67 (2022), <http://ssrn.com/abstract=3939898>.

¹⁵⁷ RACHEL CARSON, *SILENT SPRING*, HOUGHTON MIFFLIN CO., (1962); see also Scott J. Shackelford, Anjanette Raymond, Martin A. McCrory & Andrea Bonime-Blanc, *Cyber Silent Spring: Leveraging ESG+T Frameworks and Trustmarks to Better Inform Investors and Consumers about the Sustainability, Cybersecurity, and Privacy of Internet-Connected Devices*, U. PA. J. BUS. L. 505 (2023), <https://ssrn.com/abstract=4003576>.

¹⁵⁸ Press Release, United Nations General Assembly, Only 11 Years Left to Prevent Irreversible Damage from Climate Change, Speakers Warn During General Assembly High-Level Meeting (Mar. 18, 2019), <https://www.un.org/press/en/2019/ga12131.doc.htm> (last viewed July 7, 2021).

¹⁵⁹ Trautman & Newman, *supra* note 156.

late October 2021 meeting of the G20 in Rome found a focus and concern for global climate issues.¹⁶⁰ Just days later, the November 1, 2021 remarks of António Guterres, UN Secretary-General in Glasgow, United Kingdom at the twenty-sixth Conference of the Parties to the United Nations Framework Convention on Climate Change (COP26) stress our global survival crisis:

The six years since the Paris Agreement [on climate change] have been the six hottest years on record. Our addiction to fossil fuels is pushing humanity to the brink. We face a stark choice: either we stop it — or it stops us. In the age of interconnectivity, it is not enough to build a wall of security but rather we must look for, interrupt, and alleviate risks proactively while understanding how our risks affect others'.¹⁶¹

B. Weather Induced Disaster Management

Given recent technological advances, the IoT has the potential to become one of the most important enabling technologies for disaster management and relief.¹⁶² Sinha et al. identifies the following three major application areas of IoT in disaster management: (i) disaster risk minimization and prevention - monitoring disaster events with satellite communication, designing early warning systems, using social media for situational awareness; (ii) disaster response - real-time communication for effective and timely relief operations; and (iii) disaster recovery - online search for missing person and fund management systems. IoT can also be used to plan preventive maintenance and repairs; evaluate whether structures can withstand a coming weather event while continuing normal operations and close unsafe assets.¹⁶³ The IoT technology, having the potential for communicating instantaneous information updates, can be a key player for realizing dynamic workflow adaptations.¹⁶⁴

By mid-2022, “For India and other South Asian countries, home to hundreds of millions of humanity’s most vulnerable, a seemingly bottomless well of challenges — poverty, food security, health, governance

¹⁶⁰ Sha Hua & Max Colchester, *Coal Use Stirs Clash at Climate Summit*, WALL ST. J., Oct. 30-31, 2021, at A1.

¹⁶¹ *Id.*

¹⁶² See Akash Sinha, Prabhat Kumar, Nripendra P. Rana, Rubina Islam & Yogesh K. Dwivedi, *Impact of Internet of Things (IoT) in Disaster Management: A Task-Technology Fit Perspective*, 283 ANNALS OF OPERATIONS RESEARCH 759-794 (2019).

¹⁶³ *Id.*

¹⁶⁴ *Id.*

— has only deepened as the region bakes on the front lines of climate change.”¹⁶⁵ *The New York Times* reports:

Global warming is no longer a distant prospect that officials with short electoral mandates can choose to look away from. The increasing volatility in weather patterns means a greater risk of disasters and severe economic damage for countries already straining to increase growth and development, and to move past the pandemic’s devastation to lives and livelihoods.¹⁶⁶

C. Corporate Sustainability Goals and IoT

The growing corporate awareness of climate sustainability issues creates a demand for IoT sensory devices. IoT Analytics states “More than 300 global companies (including Mercedes-Benz, Schneider Electric, Uber, Microsoft, Unilever, and Infosys) have committed to The Climate Pledge, an Amazon-led initiative asking companies to reach net-zero carbon emissions by 2040.”¹⁶⁷ Consider:

To reach this ambitious goal, companies will need to measure and reduce carbon emissions in the coming years. Sustainability-focused use cases, such as IoT-based energy management, renewable energy management, and connected HVAC, are expected to be in high demand. Software tools are also required to measure sustainability footprints and achieve ESG goals. Extreme weather events, such as those already witnessed in early 2022 (e.g., storms and floods in Northern Europe and the UK, tropical storms in East Africa, and winter storms in the Northeastern US) will ensure climate change continues to get attention and will lead to further investments into energy efficiency and carbon neutrality to limit the effects.¹⁶⁸

D. The Age of Disinformation and Climate

The British Broadcast Company (BBC) has recently produced a documentary about the hack and leak of thousands of emails and documents

¹⁶⁵ Mujib Mashal & Hari Kumar, *Flood and Heat Waves Jolt India’s Food Supply*, N.Y. TIMES, June 15, 2022, at A4.

¹⁶⁶ *Id.*; see also Sang Jin Park, Dong Kun Lee & Sang Wook NAM, *Potential Flood Risk Analysis Considering Climate Change Impact*, 32 J. RISK MGMT. (2021), <https://ssrn.com/abstract=4007759>

¹⁶⁷ Philipp Wegner, *Global IoT Market Size Grew 22% in 2021 — These 16 Factors Affect the Growth Trajectory to 2027*, IOT ANALYTICS (March 30, 2022) (on file with authors).

¹⁶⁸ *Id.*

obtained during 2009 from computer systems of the Climatic Research Unit (CRU) at the University of East Anglica. According to the BBC:

The "Climategate" saga had a significant impact on opinion, especially in the US, maintaining an aura of doubt about the science longer than would otherwise be the case and therefore setting back efforts to deal with global warming.

But it also foretold a future in which information would be hacked, leaked and weaponized by different actors across social media and in which doubt would be encouraged and science questioned – all very modern themes in political debate and over COVID-19... it was the hack that changed the world.¹⁶⁹

E. The SEC and Environmental, Social & Governance Disclosure (ESG)

Professors Trautman and Newman report “on March 4, 2021 the SEC announced the creation of a Climate and ESG Task Force within the Division of Enforcement.¹⁷⁰ The new task force is “a Division-wide effort, with 22 members drawn from the SEC’s headquarters, regional offices, and Enforcement specialized units.”¹⁷¹ The Commission states:

Consistent with increasing investor focus and reliance on climate and ESG-related disclosure and investment, the Climate and ESG Task Force will develop initiatives to proactively identify ESG-related misconduct. The task force will also coordinate the effective use of Division resources, including through the use of sophisticated data analysis to mine and assess information across registrants, to identify potential violations.

The initial focus will be to identify any material gaps or misstatements in issuers’ disclosure of climate risks under existing rules. The task force will also analyze disclosure and compliance issues relating to investment advisers’ and funds’ ESG strategies. Its work will complement the agency’s other initiatives in this area, including the recent appointment of Satyam Khanna as a Senior Policy Advisor for Climate and ESG. As an integral component of the agency’s efforts to address these risks to

¹⁶⁹ *Was This The Hack That Changed the World*, BBC, <https://www.bbc.co.uk/programmes/articles/3SXrvZ2zW3rgSqKpBpNjyn2/was-this-the-hack-that-changed-the-world>.

¹⁷⁰ See Trautman & Newman, *supra* note 156 (citing Press Release, Securities and Exchange Commission, SEC Announces Enforcement Task Force Focused on Climate and ESG Issues (Mar. 4, 2021), <https://www.sec.gov/news/press-release/2021-42> (last viewed Mar. 19, 2023)).

¹⁷¹ *Id.*

investors, the task force will work closely with other SEC Divisions and Offices, including the Divisions of Corporation Finance, Investment Management, and Examinations.

‘Climate risks and sustainability are critical issues for the investing public and our capital markets,’ said Acting Chair Allison Herren Lee.¹⁷²

During March 2021, SEC’s Acting Chair Allison Herren Lee states “In 2010, the Commission issued an interpretative release that provided guidance to issuers as to how existing disclosure requirements apply to climate change matters.”¹⁷³ SEC Chair Lee further observes that “Since 2010, investor demand for, and company disclosure of information about, climate change risks, impacts, and opportunities has grown dramatically.”¹⁷⁴ Accordingly, about a year later on March 21, 2022, the Commission proposed rulemaking, “The Enhancement and Standardization of Climate-Related Disclosures for Investors,”¹⁷⁵ and extended the comment period until June 17, 2022. Professors Trautman and Newman provided the Commission with requested comments and have written a law journal article on the topic.¹⁷⁶

We will now turn our attention to the important topic of how IoT impacts healthcare.

VII. HEALTHCARE

Our country’s experience with Covid-19 has shown a spotlight on one of the great failings in our society, the lack of health equity... Covid-19 has exposed long standing inequities that have undermined the physical, social, economic, and emotional health of racial and ethnic minorities.

*Dr. Anthony Fauci
Commence Address
University of Maryland,
Baltimore*

¹⁷² *Id.*

¹⁷³ Press Release, Allison Herren Lee, SEC Acting Chair, Public Input Welcomed on Climate Change Disclosures, Public Statement (March 15, 2021), <https://www.sec.gov/news/public-statement/lee-climate-change-disclosures>.

¹⁷⁴ *Id.*

¹⁷⁵ The Enhancement and Standardization of Climate-Related Disclosures for Investors, 87 Fed. Reg. R 21334 (proposed Apr. 11, 2022).

¹⁷⁶ Trautman & Newman, *supra* note 156.

May 18, 2022¹⁷⁷

During recent years, “The United States devotes more of its national income to healthcare relative to other OECD countries... Between 2010 and 2019, health spending across the OECD averaged about 8.7 percent of gross domestic product (GDP) annually... [contrasted with] 16.3 percent to 17.0 percent of GDP,”¹⁷⁸ in the U.S. during the same timeframe. Unfortunately, spending more didn’t produce the best result with U.S. expenditures of “about \$11,100 per person on healthcare — the highest healthcare cost per capita across the OECD. For comparison, Switzerland was the second highest-spending country with about \$7,700 in healthcare expenses per capita, while the average for wealthy OECD countries, excluding the United States was only \$5,500 per person.”¹⁷⁹ Of considerable concern, “The United States actually performs worse in some common health metrics like life expectancy, infant mortality, and unmanaged diabetes.”¹⁸⁰

A. Medical Research

Medical research is both vastly important and an area where technological gains may provide significant benefits. For example, a group of research scientists write that “Cloud computing and... IoT provide new tools for managing multiple experiments in parallel that are remotely controlled through automation. [They] introduce a cloud-based IoT architecture that takes advantage of these tools to offer an environment where researchers can run thousands of cell culture experiments at once.”¹⁸¹ Consider:

Advances in IoT and cloud computing offer new solutions to overcome these challenges. IoT is a technology that remotely coordinates communication and management of large numbers of devices that are paired through the cloud. We recently developed affordable, open-source, internet-connected devices (“data acquisition modules”) for microscopy, electrophysiology, and multiple groups have developed microfluidic devices with

¹⁷⁷ University of Maryland Baltimore, *Dr. Anthony Fauci Keynote Commencement Speech at University of Maryland, Baltimore Class of 2022*, YOUTUBE (May 19, 2022), <https://youtu.be/vGBFU7uYYuw>.

¹⁷⁸ *How Does U.S. Healthcare System Compare to Other Countries?*, PETER G. PETERSON FOUNDATION (July 12, 2020), <https://www.pgpf.org/blog/2020/07/how-does-the-us-healthcare-system-compare-to-other-countries>.

¹⁷⁹ *Id.*

¹⁸⁰ *Id.*

¹⁸¹ David F. Parks et al., *Internet of Things Architecture for High Throughput Biology* (unpub. ms.) (July 23, 2021), <https://ssrn.com/abstract=3908772>.

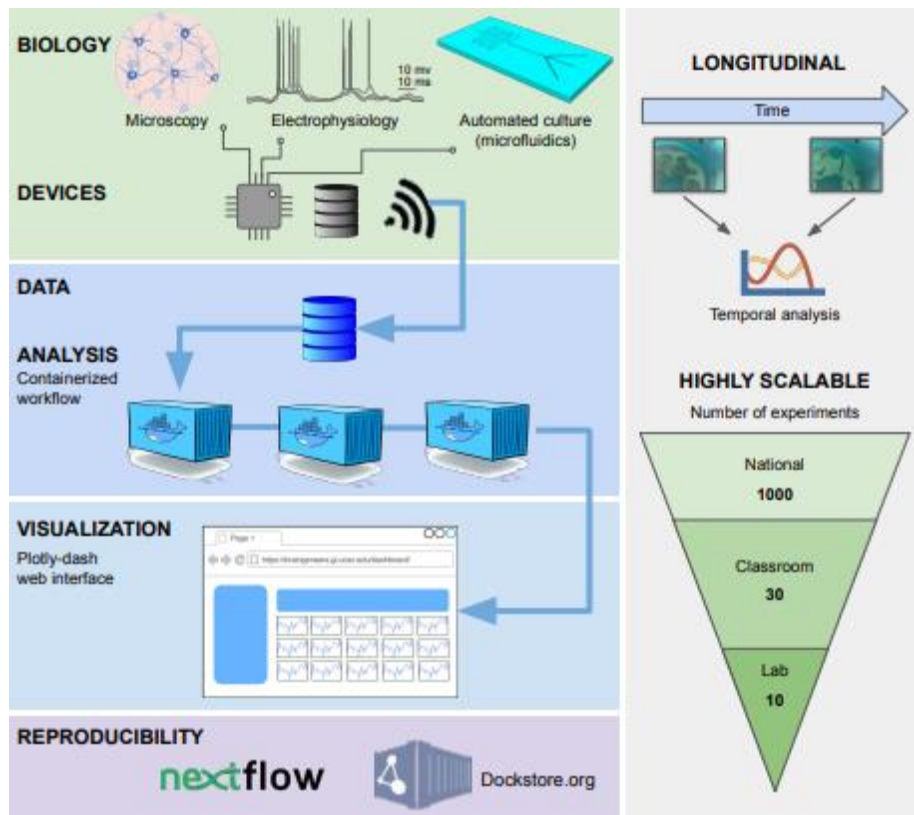
capabilities for integrated biosensors. IoT allows a globally networked fleet of lab devices to be controlled and managed through the cloud.

Cloud-controlled IoT systems enable researchers to take advantage of machine learning to optimize scientific studies. Machine learning allows IoT device to be controlled and tuned in real-time using automation. Online data streaming and analysis tools are combined with learning algorithms to create a faster turnaround between hypothesis, experiment, and re-testing. Cross comparisons of longitudinal recordings from parallel experimental replicates add new possibilities for inference. Such algorithms are easily deployed across all experiments using cloud containers. This automated environment removes batch affects between experiments, because it enforces a consistent standardized protocol.¹⁸²

Professors Parks, Voitiuk, et al. present a diagram of this IoT Cloud Laboratory and how these experiments can be automated through cloud connected devices to allow for scalability, reproducibility, and online monitoring. We have reproduced and included this illustration as Exhibit 6.

Exhibit 6

¹⁸² *Id.*

IoT Cloud Laboratory¹⁸³*B. Telemedicine*

Delivery of healthcare services via telemedicine has received a major boost as a result of the Covid-19 pandemic. Professors Sunar and Staats write “Reducing health disparities among different socioeconomic groups, thereby enhancing health equity, is the main objective of any public health policy. Telemedicine is generally seen as an important tool to reduce Health Disparities because it improves access to care by eliminating transportation barriers.”¹⁸⁴ Other scholars have discussed the benefits provided by telemedicine for renal cancer surveillance,¹⁸⁵ the use of the

¹⁸³ *Id.*

¹⁸⁴ Nur Sunar & Bradley R. Staats, *Telemedicine for Inclusive Care: Remedy for Socioeconomic Health Disparities?* (unpub. ms.) (May 8, 2022), <https://ssrn.com/abstract=4103887>.

¹⁸⁵ Adele Marie Caruso, George Lin & S. Bruce Malkowicz, *Telehealth: An Effective Model of Care for Renal Cancer Surveillance*, 18 THE JOURNAL FOR NURSE PRACTITIONERS 1086 (2022), <https://ssrn.com/abstract=4109026>.

Internet of wearable Things (IoWT) with cloud representing a major breakthrough for remote monitoring,¹⁸⁶

C. Diagnostic Facial Expressions

Professors Acquisti, Gross, and Stutzman write “Computer face recognition has been an active research topic for over forty years, alternating exciting breakthroughs with the recurrent realization that computers’ successes at recognizing people remain limited under real world conditions.”¹⁸⁷ However, during recent years, “the accuracy of face recognizers has improved so consistently that the technology has found its way into end-user products... [observing] Apple’s iPhoto has employed face recognition to identify faces in a person’s album since 2009.”¹⁸⁸ Positive IoT uses are noted and examples of IoT benefits from diagnostic applications discussed for such ailments as: Parkinson Detection;¹⁸⁹ and detection of human emotions and heart rate from analysis of facial expressions providing medical benefit.¹⁹⁰

D. Numerous IoT Healthcare Applications

The literature is full of many IoT applications for use in healthcare including: communication protocols and interface features;¹⁹¹ big data;¹⁹²

¹⁸⁶ Shadab Faham, Abdollah Salimi & Raouf Ghavami, Toward Internet of Wearable Things in Cloud-Based Telemedicine: Electrochemical-Based Remote Biomarker Monitoring (unpub. ms.) (Feb. 16, 2022), <https://ssrn.com/abstract=4004982>.

¹⁸⁷ Alessandro Acquisti, Ralph Gross & Frederic D. Stutzman, *Face Recognition and Privacy in the Age of Augmented Reality*, 6 J. PRIVACY & CONFIDENTIALITY 1, 2 (2014), <https://ssrn.com/abstract=3305312>.

¹⁸⁸ *Id.* at 3.

¹⁸⁹ Luis F. Gómez, Aythami Morales, Julian Fierrez & Juan Rafael Orozco-Arroyave, *Exploring Facial Expressions and Action Unit Domains for Parkinson Detection*, PLOS ONE (2023), <https://doi.org/10.1371/journal.pone.0281248>.

¹⁹⁰ Jagapathi babu D, Muthuraj P, Surya A & Lakshmi A, *Automated Detection of Human Emotions and Heart Rate from Facial Expressions Using PNN*, 5 INT’L J. EMERGING TECH. & INNOVATIVE ENG. (May 2019), <https://ssrn.com/abstract=3411961>.

¹⁹¹ Chun-Liang Lin, Chi-Yu Chen & Yang-Y Chen, Realization of Ideal Architecture of Iots (unpub. ms.) (Dec. 13, 2021), <https://ssrn.com/abstract=3978640>.

¹⁹² BIG DATA, HEALTH LAW, AND BIOETHICS: INTRODUCTION BIG DATA, HEALTH LAW, AND BIOETHICS, (I. Glenn Cohen, Holly Fernandez Lynch, Effy Vayena & Urs Gasser eds., 2018), <https://ssrn.com/abstract=3147243>; HENRY A. KISSENGER, ERIC SCHMIDT & DANIEL HUTTENLOCHER, *THE AGE OF AI: AND OUR HUMAN FUTURE* (Little, Brown and Company ed., 2021); Jezon Ow, The future of healthcare in Singapore. How an integrated use of A.I., Internet-of-Medical things (IoMT), Blockchain-based Technologies, and Cloud-Computing-Based Medtech and Digital Health Solutions Will Radically Address Medical Data Integrity Concerns (unpub. ms.) (Nov. 1, 2021), <https://ssrn.com/abstract=3965116>;

distributed cardiac monitoring;¹⁹³ patient monitoring;¹⁹⁴ intelligent medicine dispensing;¹⁹⁵ performance analysis on modulation techniques for medical devices;¹⁹⁶ Non-Fungible Token (NFT)-based health records;¹⁹⁷ security challenges in healthcare applications;¹⁹⁸ and mental health analytics;¹⁹⁹ just

Manikandan Sivaprakasam & Pushpa Vinu Amalraj, *Logarithmic Markle and Post Quantum Iot Based Big Data Healthcare Analysis Using Blockchain* (unpub. ms.) (Apr. 16, 2022), <https://ssrn.com/abstract=4085732>; Manisha Waghmare, Harshala Antapurkar & Shital Wagh, *I-Health-Care: Technologies Towards 5G Network for Intelligent Health-Care Using IoT Notification with Machine Learning Programming*, in PROCEEDINGS OF THE 3RD INTERNATIONAL CONFERENCE ON CONTENTS, COMPUTING & COMMUNICATION (ICCCC) (Apr. 6, 2022), <https://ssrn.com/abstract=4043870>.

¹⁹³ Ambarish G. Mohapatra, Pradyumna Kumar Tripathy, Maitri Mohanty & Ashish Khanna, *IoT Enabled Distributed Cardiac Monitoring Using Fiber Bragg Grating (FBG) Sensing Technology*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INNOVATIVE COMPUTING & COMMUNICATION (ICICC) (May 13, 2021), <https://ssrn.com/abstract=3842806>; Gilberto Andrade Tavares, Matheus Henrique Costa Xavier, Filipe Euclides Gobatto, Iara Victoria dos Santos Moura, Virna Anfrizio Souza, Wictor Hugo de Souza Silva, Gledson de Carvalho Santos, Eleonora Ferraris de Gaspare, Fabio Batista Santos, Virgílio Antônio Cardoso Faro, José Augusto Soares Barreto-Filho, *Cardiovascular Health Monitoring Mobile Phone Application Development* (unpub. ms.) (May 28, 2022), <https://ssrn.com/abstract=4122008>.

¹⁹⁴ D. Anandhavalli, N. Shanmuga Sundari, S. Aparna Tharshini, P. Pavithra & G. Sona, *Patient Health Monitoring System Using IoT Techniques*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SMART DATA INTELLIGENCE (ICSMDI) (July 22, 2021), <https://ssrn.com/abstract=3852046>; Kanubhai K. Patel, Jignesh J. Patoliya & Miral M. Desai, *IoT Based Smart Health Monitoring System with Patient Identification Using Face Recognition*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INNOVATIVE COMPUTING & COMMUNICATION (ICICC) (July 29, 2021), <https://ssrn.com/abstract=3879620>.

¹⁹⁵ Vaishali Wadhe, Kalyani Khamgaonkar, Neha Govekar, Satyakama Yerraguntala & Narmada Limbuwala, *IOT Based Patient Monitoring and Intelligent Medicine Dispensing System*, in PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON ADVANCES IN SCIENCE & TECHNOLOGY (ICAST2021) (July 12, 2021), <https://ssrn.com/abstract=3867608>.

¹⁹⁶ Yousra Lamrani, Imane Benchaib, Salma Rattal, El Miloud Ar-Reyouchi & Kamal Ghoumid, *Performance Analysis on Modulation Techniques for Medical Devices Sensitivity in Wireless NB-IoT Network*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SMART DATA INTELLIGENCE (ICSMDI 2021) (May 26, 2021), <https://ssrn.com/abstract=3852562>.

¹⁹⁷ Valli S. Kumar, John J. Lee & Qin Hu, *Non-Fungible Token-Based Health Record Marketplace* (unpub. ms.) (June 8, 2022), <https://ssrn.com/abstract=4130876>; Ochchhav S. Patel & Hiren Patel, *Ethereum Based Blockchain Technology to Achieve Confidentiality, Integrity and Access Control in Iot-Generated Healthcare Records* (unpub. ms.) (May 13, 2022), <https://ssrn.com/abstract=4109345>.

¹⁹⁸ Elisabetta Biasin & Erik Kamenjasevic, *Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals*, 3 INT'L CYBERSECURITY L. REV. 163 (2022), <https://ssrn.com/abstract=4101190>; Pothuganti, Karunakar, *Security Challenges in Internet of Things and Artificial Intelligence in*

to name a few. And, of course a considerable literature exists documenting the challenges of cybersecurity risk associated with the Medical Internet of Things (MIoT) and related pathways enabling ransomware.²⁰⁰

Next, we present a few thoughts about the important topic of IoT and regulation.

VIII. REGULATION

“Innovation doesn’t come just from updating software and hardware; it also comes from the manner in which products are offered... Beyond the innovations and technologies, our economy is changing in other ways. Today, investors are demanding additional information from companies beyond what they’ve sought historically, with respect to climate risk, human capital, and cybersecurity risk...”

Again, ‘no regulation can be static in a dynamic society.’”

Gary Gensler
Chair

U.S. Securities and Exchange Commission
January 19, 2022²⁰¹

A. Disclosure

Professors Trautman and Newman write “Disclosure of material items is at the very cornerstone of U.S. capital formation and securities regulation.”²⁰² SEC Chair Gary Gensler has stated, “We have a key role as the regulator of the capital markets with regard to SEC registrants —

Healthcare Applications, 16 INT’L J. RES. & DEV. TECH. 77 (2021), <https://ssrn.com/abstract=3944800>.

¹⁹⁹ Divya Gupta, MPS Bhatia & Akshi Kumar, *Real-Time Mental Health Analytics Using IoMT and Social Media Datasets: Research and Challenges*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INNOVATIVE COMPUTING & COMMUNICATION (ICICC) (2021), <https://ssrn.com/abstract=3842818>.

²⁰⁰ George W. Jackson, Jr. & Shawon S. M. Rahman, *Exploring Challenges and Opportunities in Cybersecurity Risk and Threat Communications Related to the Medical Internet of Things (MIoT)*, 11 INT’L J. NETWORK SECURITY & APPLICATIONS (IJNSA) (2019), <https://ssrn.com/abstract=3851799>.

²⁰¹ Gary Gensler, Chair, U.S. Securities and Exchange Commission, Prepared Remarks: “Dynamic Regulation for a Dynamic Society” Before the Exchequer Club of Washington, D.C. (Jan. 19, 2022).

²⁰² Lawrence J. Trautman & Neal F. Newman, *A Proposed SEC Cyber Data Disclosure Advisory Commission*, 50 SEC. REG. L.J. 199 (2022), <http://ssrn.com/abstract=4097138>.

ranging from exchanges and brokers to advisers and public issuers. Cyber relates to each part of our three-part mission, and in particular to our goal of maintaining orderly markets.”²⁰³ In addition, the Commission has, “many rules that implicate cyber risk, including but not limited to business continuity, books and records, compliance, disclosure, market access, and antifraud. Our Division of Examinations (EXAMS) has put out various Risk Alerts and statements regarding cybersecurity topics and issued a report in 2020 on Cybersecurity and Resiliency Observations.”²⁰⁴ Chairman Gensler states that the work of the Commission assists both SEC registrants and the public in preparation for and management of these cyber risks.²⁰⁵

B. The SEC and Data

During 2022, SEC chair Gary Gensler warns “The economic cost of cyberattacks is estimated to be at least in the billions, and possibly in the trillions, of dollars. Hackers have attacked broker-dealers, governmental agencies, meat processors, and pipelines. These attacks can take many forms from denials-of-service to malware to ransomware.”²⁰⁶ By 2022, a broad recognition that the pervasive threat of cyberattack from international criminal organizations, nation states, and even poorly capitalized criminal elements constitute a clear and present danger.²⁰⁷ During March 2022 the SEC issued a proposed rule addressing Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,²⁰⁸ to require:

1. Current reporting about material cybersecurity incidents;
2. Periodic disclosures about a registrant’s policies and procedures to identify and manage cybersecurity risks;
3. Management’s role in implementing cybersecurity policies and procedures;

²⁰³ Gary Gensler, Chair, U.S. Securities and Exchange Commission, Remarks on Cybersecurity and Securities Laws at the Northwestern Pritzker School of Law (Jan. 24, 2022), <https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124> (last viewed Feb. 19, 2022).

²⁰⁴ *Id.*

²⁰⁵ *Id.*

²⁰⁶ *Id.*

²⁰⁷ See Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?*, 18 N.C. J. L. & TECH. 232 (2016), <http://ssrn.com/abstract=2711059>; Mohammed T. Hussein, Lawrence J. Trautman, Louis Ngamassi & Mason J. Molesky, *Climate, Cyber Risk, and the Promise of The Internet of Things (IoT)* (unpub. ms.) (Jan. 7, 2022), <http://ssrn.com/abstract=3969506>; Lawrence J. Trautman, *Bitcoin, Virtual Currencies and the Struggle of Law and Regulation to Keep Pace*, 102 MARQ. L. REV. 447 (2018), <https://ssrn.com/abstract=3182867>.

²⁰⁸ Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (Mar. 23, 2022) [hereinafter “Proposed Rule”].

4. Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk;
5. Registrants to provide updates about previously reported cybersecurity incidents in their periodic reports; and
6. Cybersecurity disclosures to be presented in Inline extensible Business Reporting Language ("Inline XBRL").²⁰⁹

C. *The Corporate Governance Challenge*

Professor Seletha Butler observes "that corporations are creatures of state corporate law and related governing documents. She states that only the board itself can act on behalf of and bind the corporation, not each individual director acting independently. Directors are elected by shareholders. Subject to statutory limitations, the articles/certificate of incorporation or bylaws..."²¹⁰ Professor Butler states "In sum, the legal duties and responsibilities of directors include duties of loyalty, care, and good faith, and are subject to the "business judgment rule." She provides the following summary:

A. *Duty of Loyalty*

The corporate duty of loyalty is the obligation to subordinate personal interests to the welfare of the corporation, which includes: no competition with the corporation; not engaging in conflict-of-interest transactions (unless a majority of the disinterested directors approve the transaction after full disclosure from the interested director); no illegal insider trading; no usurpation of corporation opportunities; and no transaction that is detrimental to the minority shareholders.²¹¹

B. *Duty of Care*

At its core, the duty of care is the obligation to act in good faith and in the best interest of the corporation, which includes: making an informed and reasonable decision (i.e. performing due diligence before making a decision); if expertise is needed, engage and rely on competent consultants and experts; exercising reasonable supervision over officers; and confidentiality. Professor Butler notes "a dissenting director that has his or her dissent recorded in the minutes is rarely held liable for breach of duty of care on

²⁰⁹ *Id.*

²¹⁰ Lawrence J. Trautman, Seletha Butler, Frederick R. Chang, Michele Hooper, Ron McCray & Ruth Simmons, *Corporate Directors: Who They Are, What They Do, Cyber and Other Contemporary Challenges*, 70 *BUFF. L. REV.* 459 (2022), <http://ssrn.com/abstract=3792382>.

²¹¹ *Id.* at 466.

that applicable action.”²¹²

C. *Business Judgment Rule*

The Business Judgment Rule (BJR) is the principle pursuant to which a director or officer is immunized from liability for consequences of a business decision that turns negative as long as the decision was reasonable, informed, made in good faith, and in the best interest of the corporation. The BJR arises from the general view that informed directors acting in a manner consistent with the above are better informed and in a superior position to determine what is in the corporation’s best interest. Accordingly, only when officers or directors fail to meet the duty of care or duty of loyalty will they be held personally liable.²¹³

The duty of care applies across director’s and officers’ myriad responsibilities, including handling the corporation’s digital data. The duty of care is substantially procedural. During recent years, increased focus has been brought to bear on the responsibility of directors to ensure the data privacy of customers and users.²¹⁴ NIST observes:

Many organizations are not necessarily aware they are using a large number of IoT devices. It is important that organizations understand their use of IoT because many IoT devices affect cybersecurity and privacy risks differently than conventional IT devices do. Once organizations are aware of their existing IoT usage and possible future usage, they need to understand how the characteristics of IoT affect managing cybersecurity and privacy risks, especially in terms of risk response—accepting, avoiding, mitigating, sharing, or transferring risk.²¹⁵

D. *Duty to Provide Data Security*

Professors Trautman and Ormerod contend that the broad Duty of Care includes a duty to provide data security. Accordingly:

²¹² *Id.* at 466.

²¹³ *Id.* at 466-7; see also H. Justin Pace & Lawrence J. Trautman, *Mission Critical: Caremark, Blue Bell, and Director Responsibility for Cybersecurity Governance*, 2022 WIS. L. REV. 887 (2022), <https://papers.ssrn.com/abstract=3938128>; see also H. Justin Pace & Lawrence J. Trautman, *Climate Change and Caremark Doctrine, Imperfect Together*, 25 U. PA. J. BUS. L. 777 (2023), <http://ssrn.com/abstract=4202412>.

²¹⁴ See H. Justin Pace & Lawrence J. Trautman, *Financial Institution D&O Liability After Caremark and McDonald’s*, 76 RUTGERS U. L. REV. 449 (2024), <http://ssrn.com/abstract=4566471>; Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis*, 20 PITT. J. TECH. L. & POL’Y (2020), <http://ssrn.com/abstract=3363002>.

²¹⁵ See Bökle *supra* note 118 at iv.

The duty of care applies across directors' and officers' myriad responsibilities, including handling the corporation's digital data. There is, therefore, an emerging specific application of the duty of care as related to information technology: the duty to secure data. The applicable standard of care requires directors "to provide 'reasonable' or 'appropriate' physical, technical, and administrative security measures to ensure the confidentiality, integrity, and availability of corporate data."²¹⁶

There is not, however, a single source—such as a comprehensive federal statute or regulation—that imposes a duty to provide data security. Rather, corporate legal obligations to implement data security systems are "set forth in an ever-expanding patchwork" of state, federal, and international statutes; regulations; enforcement actions; and common law duties, including "contractual commitments, and other expressed and implied obligations to provide 'reasonable' or 'appropriate' security for corporate data."²¹⁷

Although not necessarily from a corporate governance context, many scholars have written about IoT regulation, with reference to: data portability;²¹⁸ differences in international regulation;²¹⁹ internet governance of media platforms;²²⁰ knowledge and risk management;²²¹ privacy rights²²² robots;²²³ and censored surveillance.²²⁴

²¹⁶ THOMAS J. SMEDINGHOFF, INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE 29 (IT Governance Publishing ed., 2008).

²¹⁷ See Trautman & Ormerod, *supra* note 33, (citing *Id.* at 29; see also Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who & How It Works*, 5 J. L. & CYBER WARFARE 147 (2016), <http://ssrn.com/abstract=2638448>).

²¹⁸ Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335 (2013), <https://ssrn.com/abstract=2159157>; Sarah Turner, July Galindo Quintero, Simon Turner, Jessica Lis & Leonie Maria Tanczer, *The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment*, 23 NEW MEDIA & SOCIETY 2861 (2021), <https://ssrn.com/abstract=3931040>.

²¹⁹ Lyria Bennett Moses, Richard Buckland, Benjamin James Di Marco, Anton N. Didenko, Hassan Habibi Gharakheili, Kayleen Manwaring, Jessemyn Modini, Rob Nicholls, Nigel Phair, Simon M. Taylor & Shengshi Zhao, *Submission on Australia's Cyber Security Regulations and Incentives* (UNSW Law Research Paper No. 21-85, 2021), <https://ssrn.com/abstract=4066114>.

²²⁰ Terry Flew, Professor, University of Sydney, Keynote Presentation to Media Platformization and Small Nations: The Challenge of Media Platform Regulation for Small and Medium-Sized Nations (Oct. 28, 2021), <https://ssrn.com/abstract=3951610>.

²²¹ Mohammad Ali Alqudah & Leyla Muradkhanli, *Internet of Things in Knowledge Management in E-Government*, 2 INT'L J. OF ENGINEERING AND ARTIFICIAL INTELLIGENCE 73 (2021), <https://ssrn.com/abstract=3992316>; see also NIST, *Just Released! Risk Management in the Enterprise: NIST SP 800-221 & NIST SP 800-221A* (Nov. 17, 2023),

E. Leadership at the Top

Defending against cyberattacks requires a commitment from top management to clearly communicate that good cyber hygiene is important and a top priority, not just empty rhetoric. Organizations must provide adequate resources if realistic progress against cyberthreat is to be made. Cyber-attack and data theft is a real threat for all organizations: large

<https://www.nist.gov/news-events/news/2023/11/just-released-risk-management-enterprise-nist-sp-800-221-nist-sp-800-221a> (last viewed Nov. 24, 2023).

²²² Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski & Maša Galič, *A Typology of Privacy*, 38 U. PA. J. INT'L L. 483 (2017), <https://ssrn.com/abstract=2754043>; Tiffany Li, *Privacy As/And Civil Rights*, 36 BERKELEY TECH. L.J. 1265 (2022), <https://ssrn.com/abstract=3851404>; David F. Lindsay, Genevieve Wilkinson & Evana Wright, *Regulating to Protect Security & Privacy in the Internet of Things (IoT): Draft Report*, AUSTRALIAN COMMUNICATIONS CONSUMER ACTION NETWORK (Feb. 11, 2022), <https://ssrn.com/abstract=4052068>; Bjorn Lundqvist, *Regulating Competition and Property in the Digital Economy – The Interface Between Data, Privacy, Intellectual Property, Fairness and Competition Law* (Stockholm University Research Paper No. 54, 2018), <https://ssrn.com/abstract=3103870>; Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, HARV. INT'L L.J. (forthcoming 2014), <https://ssrn.com/abstract=2418485>; Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877 (2014), <https://ssrn.com/abstract=2271442>; Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, MINN. J. L. SCI. & TECH. (forthcoming 2011), <https://ssrn.com/abstract=1656494>; Daniel J. Solove, *A Brief History of Information Privacy Law*, in PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE (Kirsten J. Mathews ed., 2016), <https://ssrn.com/abstract=914271>; Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975 (2023), <https://ssrn.com/abstract=4024790>; Allyson Haynes Stuart, *A Right to Privacy for Modern Discovery*, 29 GEO. MASON L. REV., <https://ssrn.com/abstract=3930199>; Lachlan Urquhart, Tom Lodge & Andy Crabtree, *Demonstrably Doing Accountability in the Internet of Things*, 27 INT'L J. L. & INFO. TECH. (2018), <https://ssrn.com/abstract=3087399>; W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. LAW. 221 (Winter 2016/2017), <https://ssrn.com/abstract=2894571>; Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, COLUM. BUS. L. REV. (2019), <https://ssrn.com/abstract=3248829>.

²²³ Neil M. Richards & William D. Smart, *How Should the Law Think About Robots?*, ROBOT LAW 3 (2016), <https://ssrn.com/abstract=2263363>; Kristen Thomasen, *Robots, Regulation, and the Changing Nature of Public Spaces*, 51 OTTAWA L. REV. 275 (2020), <https://ssrn.com/abstract=3535658>.

²²⁴ Janine S. Hiller, Gerlinde Berger-Walliser & Aaron Brantly, *Critical Protection for the Network of Persons*, 25 J. L. & SOCIAL CHANGE 115 (2022), <https://ssrn.com/abstract=3952121>.

corporate entities;²²⁵ educational institutions;²²⁶ entrepreneurial start-ups;²²⁷ municipalities;²²⁸ as well as non-profits.²²⁹

F. Board Talent, Experience, and Committees

Board nominating committees are challenged with the task of locating and recruiting directors who have the skills and experience necessary to govern data and information systems risk.²³⁰ Unfortunately, very few directors have a background in computer science or electrical engineering. Accordingly, many boards are frustrated by the task of governing something they know very little about.²³¹ Recent proposals, if adopted, will require disclosure of whether a board has such cybersecurity talent represented.²³² Corporate boards operate through committees. Ensuring that the enterprise has a robust defense against cyberattack is often handled by the board's audit committee.²³³ Other boards have created a risk committee with data security being an increasing focus for many organizations.

G. Recent Regulatory Update

NIST has placed a priority on assisting IoT data users in the adoption of “algorithms designed to protect data created and transmitted by

²²⁵ See Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance*, 13 HASTINGS BUS. L.J. 275 (2017), <http://ssrn.com/abstract=2623219>.

²²⁶ David D. Schein & Lawrence J. Trautman, *The Dark Web and Employer Liability*, 18 COLO. TECH. L.J. (2020), <http://ssrn.com/abstract=3251479>.

²²⁷ See Lawrence J. Trautman, Anthony “Tony” Luppino & Malika S. Simmons, *Some Key Things U.S. Entrepreneurs Need to Know About the Law and Lawyers*, 46 TEXAS J. BUS. L. 155 (2016), <http://ssrn.com/abstract=2606808>.

²²⁸ Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J. L. TECH. & POL'Y 341 (2015), <http://ssrn.com/abstract=2548561>.

²²⁹ See Lawrence J. Trautman & Janet Ford, *Nonprofit Governance: The Basics*, 52 AKRON L. REV. 971 (2018), <https://ssrn.com/abstract=3133818>.

²³⁰ See Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment*, 11 FLA. ST. U. BUS. REV. 75 (2012), <http://www.ssrn.com/abstract=1998489>.

²³¹ See Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?*, 11 DEPAUL BUS. & COMM. L. J. 205 (2013), <http://www.ssrn.com/abstract=2137747>.

²³² Trautman & Newman, *supra* note 202.

²³³ *Id.*; see also Hon. Bernice Donald, Brian Elzweig, Neal F. Newman, H. Justin Pace & Lawrence J. Trautman, *Crisis at the Audit Committee: Challenges of a Post-Pandemic World*, REV. BANKING & FIN. L. (forthcoming), <http://ssrn.com/abstract=4240080>.

the Internet of Things and other small electronics.”²³⁴ During mid-2023, NIST releases additional guidance about secure software development (SSDF).²³⁵ On July 18, 2023, the White House announced “next steps for the Cybersecurity Labeling Program for Smart Devices to Protect American Consumers, referred to as the ‘U.S. Cyber Trust Mark... defining cybersecurity requirements for consumer-grade routers.”²³⁶

We now turn our attention to an examination of IoT’s impact on “smart cities.”

IX. SMART CITIES

Cities are the most vibrant centres of human energy and creativity. They are at the nexus of new ideas, innovation and the knowledge economy. Moreover, cities are at the leading edge of efforts to address the challenges of climate change, and it is in cities that initiatives of the new green economy are being piloted.

Sha Zukang

Under-Secretary-General,

Secretary-General for the Conference

*on Sustainable Development (Rio+20)*²³⁷

IoT applications may provide cost-effective solutions for many of the problems facing municipal managers. In many cities it is evident that a considerable portion of American infrastructure is now beyond its useful life and in disrepair. A recent report from the Harvard Kennedy School contends that U.S. “current repairs and replacements are disorganized and patchwork, resulting in unsafe, costly, and inequitable roads, bridges, dams, sidewalks, and water systems. A strategic, smart infrastructure plan that integrates digital technology, sensors, and data not only addresses these

²³⁴ NIST Selects ‘Lightweight Cryptography’ Algorithms to Protect Small Devices, NIST (Feb. 7, 2023), <https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices>. (last viewed Nov. 24, 2023).

²³⁵ SSDF and IoT Cybersecurity Guidance: Building Blocks for IoT Product Security, NIST (June 22, 2023), <https://www.nist.gov/blogs/cybersecurity-insights/ssdf-and-iot-cybersecurity-guidance-building-blocks-iot-product>. (last viewed Nov. 24, 2023).

²³⁶ NIST Cybersecurity for IoT Program: Consumer IoT Security, NIST <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/consumer-iot-cybersecurity>. (last viewed Nov. 24, 2023).

²³⁷ United Nations, Bureau International des Expositions, Shanghai 2010 World Exposition Executive Committee, SHANGHAI MANUAL: A GUIDE FOR SUSTAINABLE URBAN DEVELOPMENT OF THE 21ST CENTURY, <https://sdgs.un.org/sites/default/files/publications/shanghaimanual.pdf>.

issues but can mitigate risks and even improve... our daily lives.”²³⁸ Professor Goldsmith, et al. contend “By applying data analysis to intelligent infrastructure, which integrates digital technology and smart sensors, we can identify issues with the country’s roadways, buildings, and bridges before they become acute dangers.”²³⁹ Consider:

First, by identifying infrastructure weaknesses, smart infrastructure systems can address decades of deferred maintenance, a practice that has left many structures in perilous conditions. Sensors in pavement, bridges, vehicles, and sewer systems can target where these problems exist, allowing governments to allocate funding toward the neediest projects. From there, these sensors and other smart technologies will alert leaders to changes or issues before they pose a danger—and often before a human inspector can even see them. The many infrastructure emergencies in the U.S. cost thousands of lives and billions of dollars each year, so identifying and fixing these issues is a pressing security issue. Further, as the changing climate leads to more extreme weather and natural disasters, the safety and resiliency of the country’s infrastructure is an immediate concern. Sensor systems and other intelligent infrastructure technology can identify and mitigate these problems, saving money and lives. In addition, intelligent infrastructure can be layered onto existing infrastructure to address public health concerns, like monitoring sewer water for COVID-19 and other pathogens or installing smart sensors along dangerous interstates to automatically lower speed limits and reduce accidents. It can also be used to improve materials, like concrete, to reduce the carbon footprint of a project, ultimately contributing to better health and environmental outcomes. Finally, addressing inequities is a major reason to utilize intelligent infrastructure.²⁴⁰

In many ways cities represent a unique platform where IoT technologies may be deployed to achieve a compelling return-on-investment. Because “projections from the United Nations[are] that nearly seventy percent of the world’s population may reside in urban settings by 2050, promoting sustainable development and human well-being will

²³⁸ Stephen Goldsmith, Betsy Gardner & Jill A. Jamieson, *Toward a Smarter Future: Building Back Better with Intelligent Civil Infrastructure: Smart Sensors and Self-Monitoring Civil Works*, ASH CENTER FOR DEMOCRATIC GOVERNANCE AND INNOVATION (Sept. 2021), <https://ssrn.com/abstract=3921056>. See also Beatriz Botero Arcila, *The Place of Local Government Law in the Urban Digital Age* (May 17, 2021), <https://ssrn.com/abstract=3848202>.

²³⁹ *Id.*

²⁴⁰ *Id.*

increasingly revolve around the capacities of local and regional governments.”²⁴¹ Several “smart city” case studies are found in the literature, including: the Greater Phoenix Smart Region Consortium²⁴² and Pittsburgh.²⁴³ Professor Michael Madison writes about “how smart city governance builds and relies on institutionalized sharing of data, information, and other forms of knowledge across all sectors of public administration.”²⁴⁴ Professors Gade and Aithal discuss common smart city goals such as “producing [a] lower carbon footprint, lower harmful gas emissions, and lower consumption of power... [while addressing] traffic congestion, water scarcity, energy deficiency, waste management, poor participation of citizens in city administration, maintenance of complex IT infrastructure, and so on.”²⁴⁵ Others have discussed smart cities and: blockchain;²⁴⁶ carpooling optimization;²⁴⁷ city-based public health;²⁴⁸ data-driven regulation;²⁴⁹ developing countries;²⁵⁰ disability;²⁵¹ emerging

²⁴¹ Walter G. Johnson & Diana M. Bowman, *Partnering with Non-State Actors to Govern Nexus Problems and Promote Climate Action in Smart Cities and Regions*, 62 JURIMETRICS J. 111 (2022), <https://ssrn.com/abstract=4090922>.

²⁴² *Id.*

²⁴³ Michael J. Madison, *The Kind of Solution a Smart City Is: Knowledge Commons and Postindustrial Pittsburgh*, in GOVERNING SMART CITIES AS KNOWLEDGE COMMONS (Brett M. Frischmann, Michael J. Madison, and Madeline R. Sanfilippo eds., 2022), <https://ssrn.com/abstract=4097059>.

²⁴⁴ *Id.*

²⁴⁵ Dipak Gade & P. S. Aithal, *ICT and Digital Technology Based Solutions for Smart City Challenges and Opportunities*, 6 INT’L J. APPLIED ENGINEERING & MGMT. LETTERS (IJAEML) 1 (2022), <https://ssrn.com/abstract=4038948>.

²⁴⁶ Tanweer Alam, *Blockchain-Based Big Data Integrity Service Framework for IoT Devices Data Processing in Smart Cities*, MINDANAO J. SCI. & TECH. (2021), <https://ssrn.com/abstract=3869042>; Jason Potts, Ellie Rennie & Jake Goldenfein, *Blockchains and the Crypto-City*, 59 IT - INFORMATION TECHNOLOGY 285 (2017), <https://ssrn.com/abstract=2982885>.

²⁴⁷ Shiliang Cui, Kaili Li, Luyi Yang & Jinting, Wang, *Slugging: Casual Carpooling for Urban Transit*, 24 MANUFACTURING & SERVICE OPERATIONS MANAGEMENT 2516 (2022), <https://ssrn.com/abstract=3441901>.

²⁴⁸ Himanshu Grover, *Public Risk Perception of Covid Transmission and Support for Smart Growth Policies in Seattle Metro Region* (unpub. ms.) (June 3, 2022), <https://ssrn.com/abstract=4122786>.

²⁴⁹ Sofia Ranchordas, Abram Klop, *Data-Driven Regulation and Governance in Smart Cities*, in RESEARCH HANDBOOK ON DATA SCIENCE AND LAW (A. Berlee, V. Mak, E. Tjong Tjin Tai eds., 2018), <https://ssrn.com/abstract=3126221>; Sofia Ranchordas & Catalina Goanta, *The New City Regulators: Platform and Public Values in Smart and Sharing Cities*, 36 COMP. L. & SEC. REV. (2020), <https://ssrn.com/abstract=3468194>; IGOR CALZADA, *EMERGING DIGITAL CITIZENSHIP REGIMES: POSTPANDEMIC TECHNOPOLITICAL DEMOCRACIES* (Emerald Publishing Limited ed., 2022); IGOR CALZADA, *SMART CITY CITIZENSHIP* (Elsevier ed., 2021).

technologies and sustainability;²⁵² the importance of IoT to cities in the distributed energy generation process;²⁵³ facial recognition;²⁵⁴ human rights;²⁵⁵ information and communication technologies;²⁵⁶ Latin American cities social risk;²⁵⁷ policing;²⁵⁸ privacy;²⁵⁹ security;²⁶⁰ sensor-based public health risk governance;²⁶¹ Sidewalk Toronto;²⁶² transparency and community;²⁶³ smart grid and operations management;²⁶⁴ smart tourism and

²⁵⁰ Si Ying Tan & Araz Taeihagh, *Smart City Governance in Developing Countries: A Systematic Literature Review*, 12 SUSTAINABILITY 899 (2020), <https://ssrn.com/abstract=3526607>.

²⁵¹ Samuel R. Bagenstos, *Towards an Urban Disability Agenda*, 47 FORDHAM URBAN L.J. 1335 (2020), <https://ssrn.com/abstract=3661665>.

²⁵² Suneel Kumar, Kamlesh Attri, & Varinder Kumar, *Impact of Emerging Technologies in the Development of Smart and Sustainable Cities*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INNOVATIVE COMPUTING & COMMUNICATION (ICICC) (2022), <https://ssrn.com/abstract=4024136>.

²⁵³ Yael R. Lifshitz, *Energy Cities*, in GLOBAL SUSTAINABLE CITIES (Katrina Wyman and Danielle Spiegel-Feld eds., 2022), <https://ssrn.com/abstract=4006025>.

²⁵⁴ Jathan Sadowski & Frank A. Pasquale, *The Spectrum of Control: A Social Theory of the Smart City*, 20 FIRST MONDAY (2015), <https://ssrn.com/abstract=2653860>.

²⁵⁵ Martha F. Davis, *Get Smart: Human Rights and Urban Intelligence*, 47 FORDHAM URBAN L.J. 971 (2020), <https://ssrn.com/abstract=3662390>.

²⁵⁶ Amitrajeet A. Batabyal & Hamid Beladi, *The Optimal Provision of Information and Communication Technologies in Smart Cities*, 147 TECH. FORECASTING & SOCIAL CHANGE 216 (2019), <https://ssrn.com/abstract=3439677>.

²⁵⁷ Beatriz Botero Arcila, *Latin American Cities in the Fourth Industrial Revolution: The Potential and Social Risks of Smart-Cities Technologies*, HARVARD KENNEDY SCHOOL LATIN AMERICAN POLICY JOURNAL, (Apr. 2019), <https://ssrn.com/abstract=3653493>.

²⁵⁸ Elizabeth E. Joh, *Policing the Smart City*, 15 INT'L J. LAW IN CONTEXT 177 (2019), <https://ssrn.com/abstract=3189089>; Steven Friedland, *The Digital Architectures of 'Smart' Cities and the Fourth Amendment: In Response to Andrew Ferguson*, 106 IOWA L. REV. ONLINE 176 (2021), <https://ssrn.com/abstract=3923002>.

²⁵⁹ Beatriz Botero Arcila, *The Case for Local Data Sharing Ordinances*, 30 WM. & MARY BILL RTS. J. 1015 (2022), <https://ssrn.com/abstract=3817894>; Janine S. Hiller & Jordan M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, 68 HASTINGS L.J. 309 (2017).

²⁶⁰ Daniela Popescul & Laura-Diana Genete, *Data Security in Smart Cities: Challenges and Solutions*, 20 INFORMATICA ECONOMICĂ (2016), <https://ssrn.com/abstract=3295017>.

²⁶¹ Anna Berti Suman, *The Smart Transition: An Opportunity for a Sensor-Based Public-Health Risk Governance?*, 32 INT'L REV. L. COMPUTERS & TECH. (2018), <https://ssrn.com/abstract=3231194>.

²⁶² Teresa Scassa, *Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto*, TECHNOLOGY & REGULATION 44 (SPECIAL ISSUE: GOVERNING DATA AS A RESOURCE) (2020), <https://ssrn.com/abstract=3722204>.

²⁶³ Kelsey Finch & Omer Tene, *Smart Cities: Privacy, Transparency, and Community*, in CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY (Evan Selinger, Jules Polonetsky and Omer Tene eds., 2018), <https://ssrn.com/abstract=3156014>; Hazel Si Min Lim & Araz Taeihagh, *Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications*, 11 ENERGIES 1062 (2018), <https://ssrn.com/abstract=3169740>; Ira Rubinstein & Bilyana Petkova, *Governing Privacy*

hospitality;²⁶⁵ spatial data infrastructure;²⁶⁶ and ethical and privacy concerns.²⁶⁷

A. Smart Homes

Closely related to IoT applications for smart cities is that of smart homes. The literature includes: indoor localization for ambient assisted living;²⁶⁸ home automation and big data analysis;²⁶⁹ industry consortia;²⁷⁰ sensors with face recognition;²⁷¹ and rain droplet sensors.²⁷²

The past few years has demonstrated the importance of supply chains and vulnerabilities associated with a “just-in-time” inventory strategy. We now look at the importance of IoT to supply chain strategy.

in the Datafied City, 47 FORDHAM URBAN L.J. 755 (2020), <https://ssrn.com/abstract=3578199>; A. Michael Froomkin & Zak Colangelo, *Privacy as Safety*, 95 WASH. L. REV. 141 (2020), <https://ssrn.com/abstract=3555952>.

²⁶⁴ Wei Qi, Zuo-Jun Max Shen, *A Smart-City Scope of Operations Management*, 28 PRODUCTION AND OPERATIONS MANAGEMENT 393 (2018), <https://ssrn.com/abstract=3177496>.

²⁶⁵ Sultana T. Kapiki, *Smart City and IoT Technologies Enabling Smart Tourism: The Case of Greece*, in HIGHER EDUCATION IN SMART CITY TECHNOLOGIES: EUROPEAN, KAZAKH, MONGOLIAN, RUSSIAN UNIVERSITIES APPROACH (A. Brovko, O. Dolinina eds., 2021).

²⁶⁶ Sunil Kumar & Manisha Jailia, *Smart Cities with Spatial Data Infrastructure and Big Data - A Critical Review*, 3 INT’L J. ADVANCED STUD. SCI. RES. (2018), <https://ssrn.com/abstract=3319275>.

²⁶⁷ Marta Ziosi, Benjamin Hewitt, Prathm Juneja, Mariarosaria Taddeo & Luciano Floridi, *Smart Cities: Mapping their Ethical Implications*, AI & SOCIETY (2022), <https://ssrn.com/abstract=4001761>; Igor Calzada, Marc Pérez-Batlle, Joan Batlle-Montserrat, *People-Centered Smart Cities: An Exploratory Action Research on the Cities’ Coalition for Digital Rights*, 45 J. URBAN AFFAIRS 1537 (2023), <https://ssrn.com/abstract=3970112>.

²⁶⁸ Nirmalya Thakur & Chia Y. Han, *Multimodal Approaches for Indoor Localization for Ambient Assisted Living in Smart Homes*, 12 J. INFO. 114 (2021), <https://ssrn.com/abstract=3874666>.

²⁶⁹ Rita Li, Man Yi; Herru Li, Ching Yu, Cho Kei Mak & Beiqi Tang, *Sustainable Smart Home and Home Automation: Big Data Analytics Approach*, 10 INT’L J. SMART HOME, 177 (2016).

²⁷⁰ Sven Niederhöfer & Sebastian Spaeth, *Backing the Right Horse: A Study of the Effect of Membership Dynamics on Value Creation in the Smart Home Market* (Apr. 11, 2022), <https://ssrn.com/abstract=4080862>.

²⁷¹ Rohit Swain, Dhawal Raval, Archit Sen, Mohit Singh & Pradnya Kamble, *Internet of Things (IOT) Enabled Bot for Home Security*, in PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON ADVANCES IN SCIENCE & TECHNOLOGY (ICAST2021) (2021), <https://ssrn.com/abstract=3866458>.

²⁷² Yuanming Zeng, Yu Luo, Yanru Lu & Xia Cao, *Self-Powered Rain Droplet Sensor Based on a Liquid-Solid Triboelectric Nanogenerator*, 98 NANO ENERGY (2022), <https://ssrn.com/abstract=4062556>.

X. SUPPLY CHAINS

We need to be committed to making the investments required to grow our economy. And growth includes things like investing in new technologies, supporting research and development... [so that we become less]... vulnerable... to supply chain disruptions like we have seen over the past two years.

Gina Raimondo

U.S. Secretary of Commerce

March 15, 2022²⁷³

Professors Varma and Khan state “The exponential growth of Information Technology (IT) with communication technology in Supply Chain Management (SCM) is playing critical role in optimizing decisions of the supply chain network flow for achieving organizational competitiveness, improving higher service level, lowering inventory, supply chain costs and reducing electronic risks (e-risks).”²⁷⁴ IoT Analytics reports that “In 2021, ongoing (local) COVID-19 restrictions resulted in many new and severe supply chain issues, such as a lack of vessels, trucks, and shipping containers and port congestion.”²⁷⁵ *The New York Times* reports that by mid-2022, “While some clogs in the supply chain appear to be clearing, analysts say that trend may yet stall — or even reverse — in the months to come, as retailers enter a busier fall season and dockworkers on the West Coast renegotiate a labor contract.”²⁷⁶ Professors Graves, Tomlin, and Willems write “At the start of the pandemic, with the lockdowns and restrictions, our world was turned upside down. The GDP for the United States dropped dramatically in the first half of 2020... real and current-

²⁷³ Gina Raimondo, U.S. Secretary of Commerce, Remarks by U.S. Secretary of Commerce Gina Raimondo at the Ogden Lecture at Brown University (March 15, 2022), <https://www.commerce.gov/news/speeches/2022/03/remarks-us-secretary-commerce-gina-raimondo-ogden-lecture-brown-university>.

²⁷⁴ T.N. Varma & D.A. Khan, *Information Technology in Supply Chain Management*, 3 J. SUPPLY CHAIN MGMT. 35 (2014); see also David A. Bray, Peter Brooks, Stephanie Wander, John Goodman & Teresa Carlson, *Report of the Commission on the Geopolitical Impacts of New Technologies and Data*, Commission on the Geopolitical Impacts of New Technologies and Data, THE ATLANTIC COUNCIL GEOTECH CENTER (2021), <https://ssrn.com/abstract=4075200>.

²⁷⁵ Mohammed Hasen, *State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 billion Globally*, IOT ANALYTICS (May 18, 2022) (on file with authors).

²⁷⁶ Michael D. Shear & Ana Swanson, *Visiting Port of Los Angeles, Biden Casts Inflation as a Global Problem*, N.Y. TIMES, June 11, 2022, at A14.

dollar GDP both declined by more than 30% in the second quarter of 2020.”²⁷⁷ However, “With stimulus from federal payouts, the economy recovered very quickly in the second half of 2020, with the recovery continuing strongly through 2021.”²⁷⁸ By mid-2022:

By some metrics, supply chain pressures have been easing in recent weeks. The average global price to ship a 40-foot container of goods fell to \$7,370 as of June 3, [2022] down from a peak of more than \$11,000 in September, though that was still five times higher than before the pandemic began, according to the Freightos Baltic Index.

Data published by Flexport, a freight forwarding company, shows ocean delivery times to send products from China to Europe and the United States have also dipped in the last month, though they remain twice as high as they were before coronavirus appeared.

But analysts say it’s hard to tell whether these drops reflect a normal seasonal lull in shipping before retailers gear up for a busier fall season, or a bigger change for the American economy. Economists expect consumer demand for imported products to flag at some point, as the Federal Reserve raises interest rates to try to cool the economy. But, so far, appetite for household appliances, garden tools, televisions and other goods has remained fairly resilient.²⁷⁹

Even as financial markets were selling-off during the summer of 2022, digital logistics start-up PayCargo LLC successfully funded a Series C venture funding, raising \$130 million.²⁸⁰ *The Wall Street Journal* reports “PayCargo’s software helps companies facilitates and manage payments across ocean, air, rail and trucking transport modes, PayCargo’s platform allows for real-time customer reporting and invoicing, offers workflow tools for payments and reconciliation, advanced payments, and automated refunds in any currency.”²⁸¹ At a time when many venture capital firms were pulling back on funding, “The deal is the latest signal that investors are bullish on technology companies that aim to digitize new markets. In

²⁷⁷ Stephen C. Graves, Brian Tomlin & Sean P. Willems, *Supply Chain Challenges in the Post-COVID Era*, 31 PROD. & OPS. MGMT. 4319 (2022), <https://ssrn.com/abstract=4080078>.

²⁷⁸ *Id.*

²⁷⁹ Michael D. Shear & Ana Swanson, *Visiting Port of Los Angeles, Biden Casts Inflation as a Global Problem*, N.Y. TIMES, June 11, 2022, at A14.

²⁸⁰ Marc Vartabedian, *Digital Logistics Startup Taps Investment*, WALL ST. J., June 16, 2022, at B10.

²⁸¹ *Id.*

recent years, investors have pumped capital into startups that use data and analytics to improve supply-chain efficiently.”²⁸²

A. NIST and Supply Chain Risk Management

The National Institute of Standards and Technology (NIST), observes that “A vulnerable spot in global commerce is the supply chain: It enables technology developers and vendors to create and deliver innovative products but can leave businesses, their finished wares, and ultimately their consumers open to cyberattacks.”²⁸³ Consider that “When a supply chain is compromised, its security can no longer be trusted, whether it involves a chip, laptop, server, other technology, a non-electronic product, or a service.”²⁸⁴

In the United States, “NIST is responsible for developing reliable and practical standards, guidelines, tests, and metrics to help manufacturers, retailers, government agencies, and other organizations with their Cybersecurity Supply Chain Risk Management (C-SCRM).”²⁸⁵ NIST defines C-SCRM as “a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures.”²⁸⁶ NIST has provided a significant body of technical literature during recent years to assist stakeholders in the complicated task of protecting supply chains. Our discussion in this single article can achieve little more than to provide an overview given the page-count limitation afforded any single published article.

Following a several year development process that resulted in two draft versions, during May 2022, the NIST published *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, offering “guidance on identifying, assessing and responding to cybersecurity risks

²⁸² *Id.*

²⁸³ NIST Updates Cybersecurity Guidance for Supply Chain Risk Management, NIST (May 5, 2022), <https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management>.

²⁸⁴ Cybersecurity Supply Chain Risk Management Fact Sheet, NIST (May 2022), https://csrc.nist.gov/csrc/media/Projects/cyber-supply-chain-risk-management/documents/C-SCRM_Fact_Sheet.pdf.

²⁸⁵ *Id.*

²⁸⁶ JON BOYENS ET AL., NAT'L INST. OF STANDARDS & TECH., CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT PRACTICES FOR SYSTEMS AND ORGANIZATIONS (May 2022), <https://doi.org/10.6028/NIST.SP.800-161r1>.

throughout the supply chain at all levels of an organization.”²⁸⁷ NIST observes:

Managing cybersecurity risks throughout the supply chain is a complex undertaking that requires cultural transformation and a coordinated, multidisciplinary approach across an enterprise. Effective cybersecurity supply chain risk management (C-SCRM) requires engagement from stakeholders inside the enterprise (e.g., departments, processes) and outside of the enterprise (e.g., suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers) to actively collaborate, communicate, and take actions to secure favorable C-SCRM outcomes. Successful C-SCRM requires an enterprise-wide cultural shift to a state of heightened awareness and preparedness as to the potential ramifications of cybersecurity risks throughout the supply chain.

Enterprises should aim to infuse perspectives from multiple disciplines and processes (e.g., information security, procurement, enterprise risk management, engineering, software development, IT, legal, HR, etc.) into their approaches to managing cybersecurity risks throughout the supply chain. Enterprises may define explicit roles to bridge and integrate these processes as a part of an enterprise’s broader risk management activities. This orchestrated approach is an integral part of an enterprise’s effort to identify C-SCRM priorities, develop solutions, and incorporate C-SCRM into overall risk management decisions.²⁸⁸

For additional perspective, NIST provides a graphic representation of the multilevel enterprise-wide risk management process which we have reproduced as Exhibit 7.

²⁸⁷ *NIST Updates Cybersecurity Guidance for Supply Chain Risk Management*, NIST (May 5, 2022), <https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management>.

²⁸⁸ Boyens, et al., *supra* note 286 at 18.

Exhibit 7
Multilevel Enterprise-Wide Risk Management²⁸⁹



Source: NIST (2022).

NIST has also provided valuable guidance to stakeholders by virtue of the discussion about the process of developing useful C-SCRM metrics.²⁹⁰ Accordingly, NIST observes that “Enterprises typically rely on information security measures to facilitate decision-making and improve performance and accountability in their information security programs [and] can achieve similar benefits within their C-SCRM programs.”²⁹¹ With a view toward assisting the need for corporate governance of supply chain risk, NIST suggests that “enterprises should report C-SCRM metrics to their board through the ERM process.”²⁹² Exhibit 8 illustrates a process for developing metrics.

²⁸⁹ *Id.* at 22.

²⁹⁰ *Id.* at 52.

²⁹¹ *Id.*

²⁹² *Id.*; see also Lucian A. Bebchuk, Alma Cohen & Allen Ferrell, *What Matters in Corporate Governance?*, 22 REV. FIN. STUD. 783 (2009), <https://ssrn.com/abstract=593423>; Lawrence J. Trautman, *Present at the Creation: Reflections on the Early Years of the National Association of Corporate Directors*, 17 DUQ. BUS. L.J. 1 (2015), <http://ssrn.com/abstract=2296427>; Eric Biber, Sarah E. Light, J.B. Ruhl & James Salzman, *Regulating Business Innovation as Policy Disruption: From Model T to Airbnb*, 70 VAND. L. REV. 1561 (2017).

Exhibit 8
Measuring C-SCRM Through Performance Measures²⁹³



Source: NIST (2022).

This NIST schematic for developing metrics, as provided in Exhibit 10 and outlined in [NIST SP 800-55, Rev. 1] includes:

- Stakeholder Interest Identification: Identify the primary (e.g., CISO, CIO, CTO) and secondary C-SCRM stakeholders (e.g., CEO/Head of Agency, COO, CFO), and define/measure requirements based on the context required for each stakeholder or stakeholder group.
- Goals and Objectives Definition: Identify and document enterprise strategic and C-SCRM-specific performance goals and objectives. These goals may be expressed in the form of enterprise strategic plans, C-SCRM policies, requirements, laws, regulations, etc.
- C-SCRM Policies, Guidelines, and Procedure Review: Identify the desired C-SCRM practices, controls, and expectations outlined within these documents and used to guide/implement C-SCRM across the enterprise.
- C-SCRM Program Implementation Review: Collect any existing data, measures, and evidence that can provide insights used to derive new measures. These may be found in C-SCRM Plans, POA&Ms, supplier assessments, etc.
- Level of Implementation: Develop and map measures to the identified C-SCRM standards, policies, and procedures to demonstrate the program's implementation progress. These

²⁹³ Boyens, et al., *supra* note 286, at 52.

measures should be considered when rendering decisions to prioritize and invest in C-SCRM capabilities.

- C-SCRM Program Results on Efficiency and Effectiveness: Develop and map measures of C-SCRM's efficiency and effectiveness to the identified strategy and policy objectives to gauge whether desired C-SCRM outcomes are met. These measures should be considered part of policy refreshes.
- Business and Mission Impact: Develop and map measures to the identified enterprise strategic and C-SCRM-specific objectives to offer insight into the impact of C-SCRM (e.g., contribution to business process cost savings; reduction in national security risk). These measures should be considered a component of goal and objective refreshes.²⁹⁴

B. Supply Chains and Blockchain

A large number of scholars have recently written about applications of blockchain technology to various novel applications,²⁹⁵ including: Agile supply chain framework with IoT;²⁹⁶ application of smart contracts;²⁹⁷ for detecting counterfeit products in supply chain management;²⁹⁸ energy sector threats;²⁹⁹ smart supply chain;³⁰⁰ and various case studies.³⁰¹

²⁹⁴ *Id.*

²⁹⁵ Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, 6 JOURNAL OF GOVERNANCE AND REGULATION 45

(2015), <https://ssrn.com/abstract=2709713>; Sinclair Davidson, Primavera De Filippi & Jason Potts, *Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology*, ORGANIZATIONS & MARKETS: POLICIES & PROCESSES (2016), <https://ssrn.com/abstract=2811995>; Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 304 (2017), <https://ssrn.com/abstract=2959166>.

²⁹⁶ Xiang Ning Zhu, Gabrielle M. Peko, David Sundaram & Selwyn Piramuthu, *Blockchain-Based Agile Supply Chain Framework with IoT*, 24 INFORMATION SYSTEM FRONTIERS 563 (2021), <https://ssrn.com/abstract=3964381>.

²⁹⁷ Ahmed Muayad Younus, *Supply Chain Using Smart Contract Blockchain Technology in Organizational Business*, 2 EUR. J. RES. DEV. & SUSTAINABILITY 99 (2021), <https://ssrn.com/abstract=3899169>.

²⁹⁸ Jayaprasanna M.C. and Sujatha S, *A Block-Chain of Things (BcoT) Based System for Detecting Counterfeit Products in Supply Chain Management*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SMART DATA INTELLIGENCE (ICSMDI 2021) (2021), <https://ssrn.com/abstract=3852852>.

²⁹⁹ Zbysław Dobrowolski, *Internet of Things and Other E-Solutions in Supply Chain Management May Generate Threats in the Energy Sector—The Quest for Preventive Measures*, 14 ENERGIES 5381 (2021), <https://ssrn.com/abstract=3925593>.

³⁰⁰ Neda Azizi, Heliye Malekzadeh, Peyman Akhavan, Omid Haass, Shahrzad Saremi & Seyedali Mirjalili, *IoT-Blockchain: Harnessing the Power of Internet of Thing and Blockchain for Smart Supply Chain*, 21 SENSORS 6048 (2021), <https://ssrn.com/abstract=3926587>.

We now turn our attention to exploring IoT implications to the critical importance of water to the survival of humanity.

XI. WATER

Water is one of the world's most precious resources. Whether mitigating and adapting to climate change impacts, strengthening global health security, improving access to food, or securing energy resources, water is essential to addressing these issues and building a better future. Millions of people around the world lack access to safe drinking water and sanitation, and water supplies are increasingly scarce and unpredictable. And, of course, water is vital to all life on earth and to the conservation and restoration of nature. We must act to strengthen water security for all.

Antony J. Blinken
U.S. Secretary of State
March 22, 2022³⁰²

Water is the essential part of life; Human, animals and plants depends on this natural resource. Therefore, it deserves all the research time and technology that we can provide to secure and utilize the optimal usage. One of the unique approach is to utilize the use of Internet of Things (IoT) technology, as Professor Velmurugan observes:

The scarcity of clean water resources around the globe has generated a need for their optimum utilization. Internet of Things (IoT) solutions, based on the application specific sensors' data acquisition and intelligent processing, are bridging the gaps between the cyber and physical worlds. IoT based smart irrigation systems can help in achieving optimum water-resource utilization in the precision farming landscape.³⁰³

³⁰¹ Ahmed Muayad Younus & Hala Younis, Utilizing Blockchain Technology in the Supply Chain Management in New Zealand Manufacturing: The Theoretical Perspective (Dec. 11, 2021), <https://ssrn.com/abstract=3982846>.

³⁰² Press Release, Antony J. Blinken, Secretary of State, U.S. Dept. of State, World Water Day (March 22, 2022), <https://www.state.gov/world-water-day-2/>.

³⁰³ S. Velmurugan, *An IOT Based Smart Irrigation System Using Soil Moisture and Weather Prediction*, 8 INT'L J. ENGINEERING RES. & TECH. (IJERT) (2020), <https://ssrn.com/abstract=3597146>.

And of course, access and bandwidth availability differs from location to location across the globe, with professors Sathiyamoorthy and Sarathchandra observing that “Internet of Things (IoT) implementation in Sri Lanka is limited... [and] address[ing] the need of adopting IoT technology in irrigation of coconut farming in Sri Lanka to examine the situation before the IoT implementation and the benefits after the implementation of IoT.”³⁰⁴

A. Water Efficiency and Security

In discussing global water issues, U.S. Secretary of State Antony Blinken observes “Many of our goals – and those of our partners – cannot be achieved without water security. The United States is investing in water resources and infrastructure at home and abroad through the U.S. Global Water Strategy, a whole-of-government approach to advance our vision for a water-secure world.”³⁰⁵ When considering U.S. foreign policy, Secretary Blinken reports that “We are also integrating water security and water management into our climate adaptation efforts. Through our commitment to conserve 30 percent of our land and waters by 2030, we will help maintain the ecosystems that are so crucial for water security.”³⁰⁶ Professor Neha teaches:

Water efficiency is a crucial concern for every country in the globe, and various studies, such as integrated water management, have been produced to improve the management of water resources. As a result, smart water systems were created to achieve water fairness, economic benefits for both consumers and utilities, better system management, and optimum water efficiency. A prepaid water meter is a device that monitors the amount of water used by residents who have it installed in their homes. In many apartments, water conservation is a major concern.³⁰⁷

³⁰⁴ M. Sathiyamoorthy & Sarathchandra A.W.C.K., *The Investigation of Benefits and Challenges of Using IoT Technology to Enhance the Irrigation Method of Coconut Farming in Sri Lanka*, in PROCEEDINGS OF THE 12TH INTERNATIONAL CONFERENCE ON BUSINESS & INFORMATION (ICBI 2021) (2021), <https://ssrn.com/abstract=4115643>.

³⁰⁵ World Water Day, *supra* note 302.

³⁰⁶ *Id.*

³⁰⁷ Darshana Ahire Neha, *Prepaid Water Meter and Water Quality Checking Using IOT*, 10 INT’L J. OF ALL RES. EDU. & SCI. METHODS (IJARESM) (2022), <https://ssrn.com/abstract=4090134>.

Elsewhere professors Zahari, Shairi and El Pebrian write, “With emerging technologies like the Internet of Things (IoT), increasing agricultural and farming productivity is crucial to increasing yields and cost-effectiveness. IoT, in example, can increase the efficiency of agriculture and farming processes by automating tasks that previously required human interaction.”³⁰⁸ Others report use of IoT for real-time monitoring of meteorological data,³⁰⁹ for weather prediction,³¹⁰ including tsunamis.³¹¹

In the United States “Despite water scarcity, aging infrastructure, such as leaky pipes and water mains, is estimated to result in the loss of 2.1 million gallons of treated drinking water in the U.S. each year, representing approximately 14 to 18 percent (or one-sixth) of the nation’s treated water.”³¹² Professors Goldsmith, Gardner and Jamieson write:

To mitigate water stress, water resources need to be managed more effectively. The use of smart technologies can improve water resource management, which can help to abate water scarcity. For example, smart water grids are being used to improve the management and preservation of water resources, integrating technology into water infrastructure and management systems to provide a more efficient water supply network.³¹³

B. Flooding

³⁰⁸ Mohd Khairy Zahari, Noor Azwan Shairi & Darius El Pebrian, Reviews of Wireless Power Transfer (Wpt) Internet of Things (Iot) for Smart Agricultural (Apr. 30, 2022), <https://ssrn.com/abstract=4097337>; Najiya Naj & Amogh Sanzgiri, *An IoT based Real-Time Monitoring of Water Quality System*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON IoT BASED CONTROL NETWORKS & INTELLIGENT SYSTEMS - ICICNIS 2021 (2021), <https://ssrn.com/abstract=3883305>; Sai Bhatt Keshipeddi, IoT Based Smart Water Quality Monitoring System (Aug. 13, 2021), <https://ssrn.com/abstract=3904842>.

³⁰⁹ Dnyaneshwar B. Ahire, Vitthal J. Gond & Nitin L. Ahire, *IoT Based Real-Time Monitoring of Meteorological Data: A Review*, in PROCEEDINGS OF THE 3RD INTERNATIONAL CONFERENCE ON CONTENTS, COMPUTING & COMMUNICATION (ICCCC-2022) (2022), <https://ssrn.com/abstract=4043518>; Vaishnavi Lakhara, Priya Kurade, Tejaswini Pawar, Arti Chougule & Medha Asurlekar, *Real Time Weather Monitoring System Implementation Based on Internet of Things*, in PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON ADVANCES IN SCIENCE & TECHNOLOGY (ICAST2021) (2021), <https://ssrn.com/abstract=3866819>.

³¹⁰ Vijayalakshmi A., Neethu Behanan & Rakshita Ramesh, *Internet of Things and Machine Learning for Weather Prediction*, 15 IUP J. COMPUTER SCI. 20 (2021), <https://ssrn.com/abstract=3949400>.

³¹¹ Selvakumar Manickam & Yuhong Yang, Using IoT Technology to Predict Tsunami (Feb. 19, 2022), <https://ssrn.com/abstract=4038625>.

³¹² See Goldsmith, Gardner & Jamieson, *supra* note 238, at 12.

³¹³ *Id.*

Professors Kumari, Mahato, Kumar, Abhinab, Acharjee and Dutta discuss the negative impact of global flooding worldwide and conclude that “its impact on our society can be very well reduced... [by] providing early warnings to areas likely to be ravaged by flood events using Wireless Sensor Network (WSN).”³¹⁴ Other researchers report a strategy utilizing the Internet of Things (IoT) as an embedded system to provide calculations in real-time by employment of a “Wireless Sensor Network (WSN) for computational processing, prediction and analysis” to provide alert messages intended to reduce risk.³¹⁵

XII. WORKER SAFETY

The realities of our health care system are driving many health workers to burnout. They are at an increased risk for mental health challenges and choosing to leave the health workforce early. They work in distressing environments that strain their physical, emotional, and psychological well-being. This will make it harder for patients to get care when they need it.

*Dr. Vivek Murthy
U.S. Surgeon General³¹⁶*

The Internet of things (IoT) can play an important role in worker safety. Technological advances and smart sensors are the key to such innovative approaches and methods. Presented below are a few examples of current related research in the area of worker safety as illustrated by sewage environmental monitoring systems, and Augmented Reality (AR).

³¹⁴ Dolly Kumari, Leena Mahato, Golden Kumar, Goutam Kumar, Kumar Abhinab, Jaydeep Kumar, Pradip Acharjee & Arijit Dutta, *Study on IOT Based Early Flood Detection & Avoidance*, in INTERNATIONAL CONFERENCE ON RECENT TRENDS IN ARTIFICIAL INTELLIGENCE, IoT, SMART CITIES & APPLICATION (ICAISC 2020) (2020), <https://ssrn.com/abstract=3652362>

³¹⁵ Nandhini N., Lavanya N. & Kowshika V., *Flood Monitoring and Alerting System Using Arduino in IoT*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SMART DATA INTELLIGENCE (ICSMDI 2021) (2021), <https://ssrn.com/abstract=3852091>.

³¹⁶ Dr. Vivek Murthy, U.S. Surgeon General, *Healthcare Worker Burnout*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES OFFICE OF THE U.S. SURGEON GENERAL, <https://www.hhs.gov/surgeongeneral/priorities/health-worker-burnout/index.html>.

A. Sewage Environment Monitoring System

Numerous examples of IoT to provide usage and integration of applications for enhanced worker safety are noted. The obvious goal is to utilize IoT to decrease the number of injuries occurring in the workplace. Consider the utilization of IoT to monitor the safety of sewage workers, thereby assisting to reduce the instance of workplace injuries. Professors Jha, Pal, Sonkhla, Jain and Saquib Faraz write that, “The hardware of the system can be attached through a wrist band or inserting into the jacket making it wearable for the workers. This will help provide required data after which the processed data can be uploaded to the monitoring system via IoT.”³¹⁷

B. Safety of Coal Miners

Here, we see an IoT application incorporated into a wearable smart safety jacket to provide monitoring of the health condition of coal miners by incorporating sensors to measure blood pressure, Electroencephalogram, pulse, and temperature.³¹⁸

C. Augmented Reality (AR) and Worker Safety

In her discussion about how Augmented Reality can assist in worker safety applications, economist Dr. Abigail Devereaux defines AR as “a real-time, interactive user experience that inserts virtual computer-generated elements into a user’s environment.”³¹⁹ Further, “AR technology utilizes the Internet of Things (IoT) to enable smart devices to capture and identify “scenes” as a user moves through her world, generate contextually relevant holograms, sound, and other sensory inputs, then project those virtual elements through the user’s display.”³²⁰ In addition, “AR technology is coordinative in that it assists in economic calculation, aids in tracking

³¹⁷ Varsha Jha, Shashi Pal, Aayush Sonkhla, Nishthaa Jain & Mohd Saquib Faraz, *Safety Monitoring of Sewage Workers Using IOT and Machine Learning*, in PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON ADVANCES IN SCIENCE & TECHNOLOGY (ICAST2021) (2021), <https://ssrn.com/abstract=3866193>

³¹⁸ Akshad Jha, Chaitanya Kulkarni, Gauri Japkar & Vijaykumar Bhanuse, *Safety of Coal Miners Using IoT*, in PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON IoT BASED CONTROL NETWORKS & INTELLIGENT SYSTEMS - ICICNIS (2021), <https://ssrn.com/abstract=3884031>.

³¹⁹ Abigail Devereaux, *The Augmented Commons: How Augmented Reality Aids Agile Self-Organization* (GMU Working Paper in Economics No. 17-45, 2017), <https://ssrn.com/abstract=2956718>.

³²⁰ *Id.*

usage, and helps agents overcome some kinds of information asymmetries.”³²¹ Dr. Devereaux also provides examples from existing AR applications to “conceptualize how AR strengthens self-organization and enables polycentric loci of private governance to emerge... call[ed] agile self-organization:

Examples include information-enhancing overlays, automatic language translation, individualizing and privatizing the provision of personal and worker safety, reducing emergency response times, and enriching education with overlays and holograms. We conclude that AR technologies could erode traditional policy rationales for intervention and allow private governance to take hold and flourish in situations where it has traditionally had difficulty doing so.”³²²

XIII. CONCLUSION

The daily life of billions of individuals worldwide has been forever changed by IoT technology in just the last few years. Recently, the world remains mired in the aftermath following years of dealing with a highly infectious pandemic; Russia is engaged in an invasion of Ukraine; war has erupted in the Middle East; food insecurity is rapidly increasing; the World Bank and others warn of likely future economic distress; and adverse destructive weather events continue as the result of highly disruptive climate change. As we have shown throughout this paper, successfully meeting the challenge of regulation and risk management associated with IoT devices may result in functionality improvements and productivity gains that may be applied to many of our most pressing problems.

³²¹ *Id.*

³²² *Id.*