Documents to U / MNU Lending

University of Minnesota - Interlibrary Loan Lending

OCLC **MNU** * DOCLINE **MNUMIN**

DOCUMENTS To U - MINITEX
University of Minnesota
Wilson Library, Room 60
309 19th Ave South
Minneapolis, Minnesota 55455

Phone: 612-624-4388, Fax: 612-624-4508, e-mail: docstou@umn.edu

This article is delivered directly from the collections of the University of Minnesota.
Thank you for using our service.

If you have problems with delivery, please contact us within 48 hours.

PART ONE

FROM COMMUNICATION TO CONTROL

This page intentionally left blank

1

After the Internet

IF HUMANS SUDDENLY VANISHED FROM EARTH, the digital world would still vibrantly hum. Surveillance cameras scanning streets from Beijing to Washington would stream video. Self-driving trucks would haul material around an Australian mine. Russian social media bots would circulate political propaganda. Internet-connected thermostats would regulate home climates. Robots would move merchandise around massive warehouses. Environmental sensors would gauge air pollution levels. A giraffe wandering through a game reserve would trigger a motion detector that opens a gate. Bank accounts would make automatic mortgage payments. Servers would mine Bitcoin. Until electricity stops flowing, cyberspace lives.

This sounds like the prologue of a science fiction story but is just a pragmatic acknowledgment of how far digital systems have leapt from human-facing display screens into the physical world of material objects and artificial intelligence. The Internet is no longer merely a communication system connecting people and information. It is a control system connecting vehicles, wearable devices, home appliances, drones, medical equipment, currency, and every conceivable industry sector. Cyberspace now completely and often imperceptibly permeates offline spaces, blurring boundaries between material and virtual worlds.

This transformation of the Internet from a communication network between people to a control network embedded directly into the physical world may be even more consequential than the shift from an industrial society to a digital information society. The potential for human advancement and economic growth

is as staggering as the accompanying society-wide dilemmas. How will work be transformed as autonomous systems and networked objects embedded with sensors and actuators subsume entire labor sectors, from transportation to food service? Will there be any domain of human existence that remains private, or is individual privacy no longer conceivable? What does the Internet embedding into the physical world mean for consumer safety and national security?

The stakes of cybersecurity rise as Internet outages are no longer about losing access to communication and content but about losing day-to-day functioning in the real world, from the ability to drive a car to accessing medical care. The Internet of things (IoT) bleeds into the real world in ways that enhance life but also can compromise personal safety and security. The nature of war and conflict transforms as the cyber-embedded physical world can be surveilled and disrupted from anywhere on Earth. The expansion of the Internet into everyday objects is a new threat matrix for national security. Dependencies on the stability and security of cyberspace, already necessary for the digital economy and the public sphere, extend deeper into human safety and the basic functioning of material infrastructures of water, energy, and transportation systems.

Internet-connected objects bring privacy concerns into intimate spheres of human existence far beyond the already invasive data-gathering practices of Facebook, Google, and other content intermediaries. Ambient data gathering of routine activities within homes and around medical and health practices can be much more privacy invasive even than surveillance of emails, texts, websites visited, and other digital content through the clear portal of a screen. Devices collect personal information about everything humans do in daily life. It is not preordained that individual privacy will ever meaningfully be possible. Even gaining personal consent for data collection is sometimes impossible because affected individuals may not be the owners of these devices or even aware of their presence. Unprecedented privacy questions arise around what personal data is gathered and shared from everyday objects and the types of government surveillance now possible in life spheres that were previously shielded from any external scrutiny.

Three cybersecurity stories highlight the rising political stakes of this embedding of digital technologies into the material world. The first involves connected medical devices and rising concern about human safety. Former U.S. vice president Dick Cheney and his cardiologist disclosed in a television interview that the doctor had, in 2007, ordered the disabling of a wireless feature on

the vice president's implanted defibrillator in an abundance of caution around fears that a terrorist could carry out an assassination by wirelessly hacking into the pacemaker.[1] This seemed like a remote possibility until, ten years later, the U.S. Food and Drug Administration (FDA) issued a safety warning about cybersecurity vulnerabilities in radio-frequency-enabled implantable cardiac devices, including pacemakers and defibrillators.[2] The affected devices transmit data to a home monitor, which can, in turn, connect to a physician over the Internet. The FDA warning suggested that "someone other than the patient's physician" could "remotely access a patient's RF-enabled [radio-frequency-enabled] implanted cardiac device."[3] Cyber technologies are not only embedded in objects; they are embedded in objects that are embedded in the body.

The Stuxnet worm detected in 2010 similarly exemplifies political entanglements between digital and material infrastructure. Stuxnet was highly sophisticated code designed to infiltrate and sabotage the control systems operating Iranian nuclear centrifuges.[4] Stuxnet is typically described as a coordinated U.S.-Israeli initiative crafted to sabotage Iran's nuclear weapon aspirations, although neither the U.S. nor Israeli government officially acknowledges these claims.[5] Since Stuxnet, there have been countless politically motivated attacks on critical infrastructure including disruptions to the Ukrainian power distribution systems, which officials have attributed to Russian security services. These attacks demonstrate how control of cyber-physical infrastructure is now a proxy for state power.

The Mirai botnet is a similarly revealing example. This largest cyberattack in history was carried out by hijacked Internet-connected home appliances. More than eighty popular sites, including Amazon and Reddit, became inaccessible in parts of the United States in the fall of 2016. The cause of the outages was a massive distributed denial of service (DDoS) attack. The assault hijacked millions of unwitting devices, exploiting security vulnerabilities to implant malicious code and using these hijacked devices to flood the targeted sites with so many requests as to render the targets inaccessible to legitimate traffic. A real-world analogy would be millions of people simultaneously calling a 911 dispatcher. The dispatch system itself is not infiltrated, but the sheer volume of spurious calls makes the service unavailable to legitimate calls. As such, a DDoS attack has a similar effect as a complete outage of a besieged system. Tools for launching these attacks are readily and freely available online or as services available for hire.

This outage received considerable media attention because the sites affected, including Netflix and Twitter, were some of the most popular Internet services

at the time.[6] There were much more alarming characteristics that offer insights about the nature of distributed control points in virtual-material spaces. First, the attack was carried out not directly against the affected sites but by attacking an intermediary technology necessary to keep the sites operational: the Domain Name System (DNS). The DNS is a massive, globally distributed database management system whose main function is to translate human-readable domain names (e.g., Netflix.com) into unique numbers (binary Internet Protocol, or IP addresses) used to locate virtual resources online. Because the DNS is used nearly every time someone queries a name online, it is a choke point where the flow of information can be disrupted. The attack even more specifically targeted Dyn, a company that provides managed DNS services responsible for resolving queries for the domain names of some of the sites affected. Dyn's chief strategy officer described the outage as "a sophisticated, highly distributed attack involving 10s of millions of IP addresses . . . across multiple attack vectors and Internet locations."[7]

The Mirai botnet is a specific example of a general condition that control can be exerted by co-opting or disrupting intermediary infrastructures (rather than targeted systems) to achieve some objective.[8] It is not necessary to infiltrate or attack the intended site directly but only indirectly by turning to a supporting system, such as the DNS, systems of routing and addressing, cloud computing platforms, and points of network interconnection. Indeed, the DNS has long been used for information control, from political censorship to blocking access to pirated movies, and has even longer been a target of DDoS attacks.[9] These technical infrastructures have a concealed complexity and a distributed architecture that keeps them out of public view. Attacks bring visibility to this behind-the-scenes infrastructure and also highlight the crucial role of private companies as points of digital concentration and administration on which the stable exchange of information depends.

Much more consequentially, this massive attack was carried out primarily by home appliances such as security cameras and digital video recorders.[10] The botnet, short for "(ro)bot net(work)," was a collection of interconnected devices infected with malicious software (malware), without the device owners' knowledge. Consumer IoT devices are susceptible to malware because they may contain security vulnerabilities or use weak (or no) default passwords. In this instance, the Mirai botnet scanned networks for vulnerable devices and surreptitiously infected them with malicious code used to coordinate the attack. An

analysis of the attack suggested that the Mirai botnet used "a short list of 62 common default usernames and passwords to scan for vulnerable devices" and was able to access and infect mass numbers of appliances because so many people had never changed the default username and password or else used very weak passwords, like "password."[11]

The incident is also indicative of how security exploits, once developed and regardless of initial motive, can take on a life of their own. Three college-age defendants pleaded guilty to conspiring to violate the U.S. Computer Fraud and Abuse Act (CFAA) for creating and using the Mirai botnet to target connected home appliances and exploit these to execute DDoS attacks. The Department of Justice disclosed that one of the defendants "posted the source code for Mirai on a criminal forum," which others then accessed and used later to carry out attacks such as the one that disrupted major Internet content sites in the fall of 2016.[12] Media reports claimed that the motive for developing the Mirai botnet was to gain competitive advantage in the wildly popular computer game Minecraft.[13]

Connected objects are not only a potential target but also a potential threat vector from which to launch attacks. The security of popular websites and content platforms is only as strong as the security of cyber-physical systems far removed from these platforms. Their fate is intertwined. Some connected home devices are not upgradable or come with inherently weak security. In other cases, owners ignore security patches as devices become part of the taken-for-granted background edifice of daily life. Consumer objects can be weaponized when they are vulnerable to exploits, and they are increasingly within the crosshairs of those who seek to exert control across borders.

As these three examples emphasize, the design and control of connected physical objects is an emerging and high-stakes terrain of global Internet policy. Cybersecurity has now become one of the most consequential issues of the modern era, necessary for human safety, privacy, critical infrastructure, and national security, as much as for economic security, democracy, speech rights, and access to knowledge. Yet connected physical objects are notoriously insecure. There is a huge chasm between the need for security and the state of security. Realizing the improvements to human life and the economic growth possible from cyber-physical innovations is predicated upon the inherent security and stability of these systems. Technology policy must, in the contemporary context, anticipate and address future questions of accountability, risk, and who is responsible for outages, security updates, and reliability. Public policy has not yet caught up to this

technological transformation and its consequences. Meanwhile, the pace of cyber-physical innovation is accelerating.

The Dissolution of Boundaries between Virtual and Physical Worlds

The Internet has already reached a tipping point. More *objects* are now digitally connected than *people.* This phenomenon is sometimes called the "Internet of things" or "cyber-physical systems," although these dispassionate phrases dampen the remarkable reality that the real world connected by digital systems subsumes biological processes, currency, and transportation systems, not just mundane material artifacts like connected coffee machines. Already measured in billions, there will soon be on the order of 20 billion or more material objects online.[14] Anyone with multiple tablets, computers, and smartphones intuitively understands the disproportionate ratio of devices to people online, but this is only a very partial accounting. Online artifacts include everything from kitchen appliances, door locks, home alarm systems, networked weather sensors, automobiles, energy system sensors, and industrial control systems (ICS).

As with other major technological changes, expectations about this material diffusion range from efficiency promises about "smart cities" and "smart homes" to Orwellian warnings that this will be the death knell of human autonomy. To be sure, increases in object connectivity will result in new industries creating interconnected products embedded with chips, sensors, actuators, and radio-frequency identification (RFID) capability. Whether one views this as a new trend or the continuation of the Internet's meteoric growth is of no consequence. What matters is that this phenomenon will have significant implications for economic growth, individual rights, business models, and governance and that there is a moment of opportunity to shape the constitution of this future.

In the vernacular of cyber-physical systems, connected things are real-world objects that directly embed cyber elements. They simultaneously interact with the real world and the virtual world. Their primary purpose is not communication among people or individual access to information such as news, knowledge, business data, and entertainment. They are geared more toward keeping systems functional by sensing and analyzing data and autonomously controlling devices. Like other communication devices, these objects interconnect via either wireless or wired networks. Industry sectors have used terms such as "smart grids" or "sensor networks." Policymakers have adopted language such

as "smart health" and "smart cities." Consumer electronics manufacturers call this the "Internet of things." In practice, these systems often involve sensor networks detecting contextual changes such as in the environment (weather sensors) or a physical occurrence (a door opening, the delivery of a spare part in a manufacturing system, or a movement). Already millions of sensors monitor environmental conditions, industrial systems, security points, and the movement of objects. These systems also directly actuate devices, such as moving a mechanical system or activating a light switch.

Tropes related to the Internet of things are often consumer-centric, including home appliances and other domestic systems or an individual's car or other personal object. Beyond these everyday consumer objects, industry and local governments are an important constituency operating cyber-physical environments. For example, cities operate traffic control systems, utilities, street lights, transportation apps, and other systems connected directly to the public Internet or indirectly via proprietary networks with a gateway to the public Internet. Cyber-physical systems, of course, exist in the vast infrastructures underlying industrial sectors. Digitally connected sensors provide energy companies with intelligence about natural resources. Manufacturing companies use digital networks to manage the handling of materials, optimization of inventories, and control of robotic systems. Shipping companies use embedded RFID chips to track packages and vehicles and optimize delivery routes.

Digital systems are now control systems for the real world of things but also bodies. Biological systems are part of the digital object space. The Internet of things is also the Internet of self. The "thing" in the Internet of things encompasses a person's biological systems via wearable technologies, biometric identification devices, and digital medical monitoring systems for checking temperature, heart rate, or blood glucose level. Medical diagnostic and treatment systems similarly rely on Internet-connected devices.

Physical and nonphysical boundaries collapse.[15] Values are in tension. For example, strong cybersecurity is necessary to protect national security and individual privacy but increasingly intersects with the physical world and human body in a way that creates a host of new rights concerns. Strong cybersecurity is necessary for consumer protection and privacy, especially around connected medical devices. But cybersecurity also creates challenges for individual privacy because it can require the collection of biometric identification. Human authentication and identification take place through voice, facial, or movement

recognition, retinal scans, fingerprints, and other globally unique human identifiers. China and other countries with authoritarian information technology (IT) approaches are using these biometric systems as part of social control programs.

The Internet transforms from being in a user's field of cognition to being an invisible background context of everyday life. Connected objects are continuously sensing and engaged in constant interactivity. Humans no longer directly experience connectivity through a screen but through everyday objects. This diffusion of the Internet into the material world speaks to the phenomenological sense in which the Internet is receding from human view even while expanding.

A "screen" is no longer the arbiter of whether one is online or offline. This distinction has always been imprecise because one can be swept online via screens belonging to others, such as tagged in an image or recorded in the background of a YouTube video. Nevertheless, in the era in which most access was screen mediated—a computer, phone, or tablet—it was obvious when someone was "on the Internet." There was some self-awareness and some choice. The shift away from screens and into material objects further blurs this online-offline distinction. It complicates individual awareness of personal data collection because it is more behind the scenes. Human online exposure shifts from sometimes on, when interacting with a screen, to always on, via ambient objects. Active engagement with digital networks moves to passive engagement.

Those who believe they "do not have a large digital footprint" because of personal social media choices neglect to consider the reality that modern cars capture minutiae about how they drive, phones record their every movement, and grocery store affinity cards capture consumer data. Neighborhood surveillance cameras record them walking their dog. These ambient technologies bring about enormous social benefits around convenience and safety. But choice becomes complicated. At one point, picking up a device with a screen—such as a laptop or phone—was a concerted choice about how and when to be online, even if that choice involved hidden power structures that affected individual rights. Now the choice is no longer present in the same way.

Offline-online hybridized spheres penetrate into the body, the mind, and the objects and systems that collectively make up the material world. The Internet is no longer just about communication but is also no longer simply a virtual space. Conceptions of the Internet as, a priori, a communication system between people have to be dispelled.

The upsurge of systems that simultaneously embed digital and real-world components creates conditions that challenge traditional notions of Internet governance in profound ways. It no longer makes sense to view online and offline spaces as distinct spheres, either technically or politically, with the virtual world somehow separate from the real world. They are entangled.

All Firms Are Now Technology Companies

What counts as an "Internet company" or a "tech company" transforms in the context of systems that embed both digital and material components. All firms are now technology companies, not only traditional tech firms like Google but any company (e.g., Caterpillar, Ford, GE) that manufacturers cyber-embedded products or collects massive stores of digital data.

In most industry sectors—from financial services to consumer goods—firms historically have not viewed themselves as technology companies. They had a separate information technology department serving as a support structure for developing and delivering products and services to customers. This function was parallel to other types of enabling functions, such as human resources or finance. IT departments managed communication networks, email, data storage, and industry-specific information systems such as point-of-sale in retail or production and distribution systems in manufacturing. Computer networks and the public Internet were vitally integral to operations, but end products—whether a jacket or a refrigerator—did not embed computer networking as part of the product. They existed in the real world.

Conversely, "tech companies" have historically been viewed as born digital. These include information intermediaries, like Google and Baidu, which facilitate the exchange of content; network intermediaries like AT&T or Vodafone; or software and hardware companies like Microsoft and Cisco, whose core business is selling technology for use in other industries. Tech companies have also included born-digital retail companies like Amazon, which have no physical consumer retail presence but rather transactionally exist entirely online, albeit with massive back-end warehouses.

There is no longer a logical demarcation between born-digital tech companies and nontech companies. Companies that were once entirely digital are now producing material, real-world products that expeditiously leverage their massive data-processing capabilities and experience with cybersecurity. Apple,

Google, and Microsoft have all entered markets for self-driving cars. Google has been working on autonomous vehicles since 2009, for example, through its Waymo subsidiary.[16]

The shift of real-world product and service companies into the digital realm is just as significant, if not more significant, of a factor blurring this distinction between tech and nontech companies. GE now has a significant product investment in the "industrial Internet of things" geared toward transforming industries with sensors and vast data collection and analysis, as well as augmenting its traditional product line of home appliances with digital interconnection. Financial services have moved almost entirely online. Under Armour has produced digitally connected shoes. Levi's partnered with Google to offer an interactive jacket, embedding a tag in the sleeve to enable wireless connectivity to a mobile device. Automobile companies from Ford to Tesla have sought to develop autonomous vehicles embedding communications technology and massive data processing to such a degree that these are high-tech networking products as much as cars. Ford will compete with Google as much as with Toyota.

In other cases, it is impossible to assess whether a company began digitally or began in the physical world. Is Uber a tech company or a transportation company? Is Airbnb a tech company or a hotel service? These are examples of a new generation of firms that digitally facilitate real-world interactions but do not actually operate themselves in the physical world. Digital media companies bleed into the material world. Traditionally nontech companies are digitally integrated, and there is a rising breed of new companies that are neither fully offline nor fully online. It is clear that the boundary around digital media company or tech company is blurred.

The twenty-first-century phenomenon of all firms metamorphosing into technology companies has implications for technology policy. The most immediate concern involves the question of human rights in this hybridized context. The same types of civil liberties questions arising online in traditional digital media platforms—especially the privacy parameters around personal data collection and conditions of equality, discrimination, and access—now also apply, and even more so, to these contexts blending the virtual and the material. Another complication is cybersecurity. Many of the firms that are now suddenly also digital technology firms have historically less experience with cybersecurity. There are also not necessarily market inducements for strong cybersecurity or even upgradeability in quickly emerging product lines in which being first to

market is paramount. Another of many complications is that integrating cyber interconnections in material objects makes systems traverse national boundaries in ways that can complicate jurisdiction. A physical-world product, when digitally embedded, is suddenly reachable across borders by foreign intelligence and hackers.

"Internet Users" Are Not People

This entanglement of real-world objects and the cyber world complicates even the simple category "Internet user." This once clearly measurable category is rapidly changing in the context of bots and connected objects with no human display screens. The history of the Internet's success is often told through the lens of growth in users, the number of people connected via a computer, laptop, tablet, or smartphone. The International Telecommunication Union (ITU) has consistently provided global and country-specific usage statistics about human-centric categories such as percentage of individuals using the Internet and households with Internet access.[17] By this user-centric metric, Internet growth is staggering. Half the world's population came online by 2017. In the mid-1990s, when Amazon and eBay were founded, less than 1 percent of the world's population was online, with most users in the United States. Policymakers, advocacy groups, and scholars alike gauge Internet success by such usage statistics and direct policy efforts, particularly in emerging markets, accordingly. Examples include interventions to bridge the digital divide, improve broadband penetration in the developing world, and address net neutrality, an issue typically concerned entirely with last-mile Internet access to homes.

The growth in the number of individuals online and broadband penetration rates to homes have always had limitations as success metrics. Consumer-centric views of Internet growth have often not matched Internet use in practice, for example, focusing on individual social media usage more than Internet access by major industrial sectors. Even with a content-centric view of Internet usage, the bulk of Internet traffic is not communications between two people but entertainment programming, with video streaming services like Netflix, Amazon Prime Video, Hulu, and their competitors constituting more than half of Internet traffic during prime viewing hours. Furthermore, a single person might simultaneously use multiple screen-mediated devices: a phone, laptop, tablet, work computer, home computer. Does that count as one user or five?

User-centric Internet policy interventions also miss major swaths of public-interest issues that exist outside direct consumer interfaces and in deeper layers of Internet infrastructure.

Another complication is that some "people" online are actually bots. "Bot" is a term for software code that simulates human activity or automates some repetitive task. One of the dictionary definitions that *Merriam-Webster* provides is "a computer program or character (as in a game) designed to mimic the actions of a person."[18] The 1860 *Webster's Dictionary* defines bots as "a species of small worms, found in the intestines of horses."[19] Thankfully, in the digital age, it connects more to "(ro)bot." But bots actually are sometimes autonomous worms that self-propagate. DDoS attacks make use of armies of malicious bots.

Bots have had a central role in Internet tasks for decades, such as web crawlers that autonomously scour pages to index content for search engines. They provide customized music streaming and personalized weather forecasts. Botnets are key enablers of spam, whether collecting massive stores of email addresses or distributing unsolicited marketing messages. Regrettably, botnets are also a staple of cyberattacks and cybercrime. Sometimes indistinguishable from people, they generate automated emails appearing to be legitimate but designed to carry out identity theft. Sophisticated chatbots engage in conversations with people. Intelligence communities in the United States indicated that Russians used bots, as well as troll farms of actual people, to disseminate propaganda microtargeting American voters in an attempt to influence the 2016 presidential election.

Software code masked as human social media accounts produces a nontrivial percentage of social media content. They have a variety of purposes—marketing, political propaganda, influence campaigns, news dissemination, spam, hate speech, activism. But they are not individual users. One group of researchers estimated that "between 9% and 15% of active twitter accounts are bots."[20] One can simply observe the immediate aftermath of a Twitter posting by a prominent person. Within less than a second, tens of thousands of "users" retweet the message. Much of this instantaneous content generation does not originate with actual human followers but via social media message-amplification techniques. Counting "users" can include counting nonhumans. Twitter has disclosed the scale of what the company faces in dealing with automated (nonhuman) accounts: "On average, our automated systems catch more than 3.2 million suspicious accounts globally per week—more than double the amount we detected this time last

year. As our detection of automated accounts and content has improved, we're better able to catch malicious accounts when they log into Twitter or first start to create spam."[21]

The massive scale and sophistication of bot accounts make the problem impossible to address via direct human detection and intervention. Only machine learning and automated pattern-detection capabilities can address the bot tsunami flooding the digital public sphere. Scholars who study the surface of content have sometimes compounded the problem. Studying discourses in social media platform intermediaries can help propagate disinformation because it adds a veneer of quantitative legitimacy to what is actually gaming of systems.

While "Internet user" has always been an imperfect category, it is further complicated in the context of the cyber-embedded physical world. Connected objects outnumber connected people. What counts as an Internet user? Connected lighting systems and doorbells exchange data just like humans exchange data. A lightbulb is not an Internet user by traditional definition, but it might be technically more accurate to measure the number of devices online rather than the number of users online.

Many connected objects, particularly in environmental, agricultural, energy, and other industrial settings, have no formal relationship to human users and no display screen or formal user interface. Machine-to-machine, or M2M, is a significant usage category, encompassing devices in industrial settings, such as supervisory control and data acquisition (SCADA) systems or other sensing and control transactions at digital-physical borders. These devices exchange information, consume resources such as bandwidth and IP addresses, and raise all manner of cyber governance questions but are not counted as "users."

Even people who have never been online are directly affected by what happens online. Everything is connected, so everyone is affected. Phrases such as "being on the Internet" or "being off the Internet" no longer have distinct meanings. Data breaches affect non-Internet users. During a hectic 2013 holiday shopping season, the U.S. retail giant Target acknowledged that hackers gained unauthorized access to its customers' credit card numbers and other personal information. The data breach originated via an infiltration of a third-party heating, ventilation, and air conditioning system company connected to Target's network.[22] Target acknowledged that the stolen information included a customer's name, credit card number, expiration date, and card verification value (CVV) number (the three or four-digit number on a credit card), as well

as home address, email address, and phone number.[23] Identity theft is a trivial matter given this combination of personally identifiable data. The retailer suggested that the massive data breach affected as many as seventy million customers and, as companies often do in such case, offered a complementary year subscription to a credit-monitoring service for any customers who shopped in their stores.[24] A non-Internet user who shopped at Target would have been swept up in this data breach. The Office of Personnel Management (OPM) data breach in which China-based hackers gained access to the personal information of more than twenty-one million U.S. federal employees could have affected any non-Internet user who ever worked for the federal government.

Someone who buys a home alarm system but is not "online" via a traditional screen may actually be online. An elderly person simply showing up for a medical appointment can be directly affected when a ransomware attack on the health-care provider prevents the person from receiving medical care. One does not have to personally be "on the Internet" to have one's life dependent on the Internet. The category of "user" continues to evolve.

The changing user context and the expansion of what counts as a technology firm, as well as the evolution of cyber-physical technical architecture, is an important starting context for discussions about the state of Internet governance.

The Cyber-Physical Challenge to Internet Governance

What are the public-interest issues arising from the Internet's expansion from a communication network to a control network whose infrastructure is enmeshed in the material world, increasingly politicized, and involving new types of firms far beyond traditional tech companies? The pace of innovation and the opportunities for human flourishing are significant but are clearly accompanied by critical economic and social concerns.

What are the rising implications for privacy, discrimination, human security, interoperability, economic stability, and innovation? Do existing models of Internet governance still apply? Who are the new stakeholders in so-called multistakeholder governance? As the technologies become more diffuse and less visible because they are embedded in material systems, the implications of these technologies become more concealed, and choice and consent become upended. Yet the digital economy, social life, and political systems are completely dependent on the stability and security of this infrastructure.

This embedding of network sensors and actuators into the physical world has transformed the design and governance of cyber infrastructure into one of the most consequential geopolitical issues of the twenty-first century. It challenges notions of freedom and power structures in Internet governance and further blurs the role of nation-states in addressing the politics of technical structures that inherently cross borders.

For much of its history, the Internet has created connections between people or between people and information. Hence, policy formulation around the Internet, as well as theory and research, has concentrated on the network as a public sphere for communication and expression or as an information system for commercial transactions.[25] Content-centric topics have included intellectual property rights enforcement, social media influence campaigns, cyberbullying, freedom of expression, and data protection. Intellectual thought has focused primarily on this visible layer of content, communication, and transactions rather than underlying material control infrastructures.

This book seeks to make visible the power structures embedded in emerging digital-physical infrastructure landscapes, explain the social and economic stakes of how these infrastructures are designed and governed, and recommend a technology policy framework that accounts for the critical public-interest concerns arising in hybrid virtual-physical systems. The most consequential global policy concerns of the present era are arising in debates over the architecture and governance of cyber-physical systems. Technology policy has to be reconceptualized to account for the expansion of digital technologies from communication and information exchange to material sensing and control. How technical, legal, and institutional structures evolve will have sweeping implications for civil liberties and innovation for a generation.

The book is written from the standpoint of both engineering and science and technology studies (STS), and the conceptual starting point is that arrangements of technical architecture are also arrangements of power. On the contrary from implying any technological determinism, this theme suggests that those who control the design and administration of technologies shape these power structures. Technologies are culturally shaped, contextual, and historically contingent. Infrastructure and technical objects are relational concepts in that cultural and economic interests shape their composition. The philosopher of technology Andrew Feenberg has suggested that "technology is power in modern societies, a greater power in many domains than the political system

itself."[26] Interventions based on law or international agreements are not alone sufficient. Public policy is inscribed and concealed inside architecture.

Technical points of control are not neutral—they are sites of struggle over values and power arenas for mediating competing interests. At the same time, the natural and physical world, of course, exists. The scientific process and innovation incorporate facts about the physical world derived from lived material experience. From an engineering perspective, it is not possible to construct a solid rocket booster out of lawn clippings, no matter what powerful values will it so. Understanding the politics of technology requires acknowledging both material engineering realities and also the social construction of the same.

In 1980, Langdon Winner influenced a generation of scholars with his provocative essay "Do Artifacts Have Politics?" Winner suggested two ways in which artifacts could have political qualities, including how "specific features in the design or arrangement of a device or system could provide a convenient means of establishing patterns of power and authority in a given setting" and also "ways in which the intractable properties of certain kinds of technology are strongly, perhaps unavoidably, linked to particular institutionalized patterns of power and authority."[27] He was writing prior to the globalization and commercialization of the Internet or the development of the World Wide Web, but his themes would later resonate in scholarship addressing the politics of cyber technologies.

The late Susan Leigh Star described her 1999 STS publication "The Ethnography of Infrastructure" as "a call to study boring things" and suggested, "it takes some digging to unearth the dramas inherent in system design," in part because much of this work is "buried in inaccessible electronic code."[28] Star's theoretical and methodological work on infrastructure, including her work with Geoff Bowker, has helped influence a large body of scholarship in infrastructure studies, collectively "inverting" infrastructure from a background framework to the foreground to reveal underlying politics.[29] Part of the purpose of the present book is to make visible the behind-the-scenes architectural components of cyber-physical systems.

The starting point for examining the governance issues in cyber-physical infrastructure is conceptually identical to the framework from *The Global War for Internet Governance* (2014). Levers of control in Internet governance are not at all relegated to the actions of traditional governments but also include (1) the politics inscribed in the design of technical architecture; (2) the privatiza-

tion of governance, such as public policy enactment via content moderation, privacy terms of service, business models, and technological affordances; (3) the role of new multistakeholder global institutions in coordinating cross-border critical Internet resources; and sometimes (4) collective citizen action. For example, the design of technical standards is political. These are the blueprints, or specifications, that enable interoperability between products made by different companies. From the Internet Protocol to BitTorrent, technical standards are not merely technical specifications. They establish public policy in their design features that connect to national security (e.g., encryption strength), human rights (e.g., privacy-enhancing features, web accessibility standards for the disabled), and democracy (e.g., security of election support infrastructures, an interoperable public sphere, access to knowledge). Another central theme in Internet governance is the reciprocal relationship between local decisions and global networks, which can be thought of as part of control by extraterritoriality. Local regulations such as the European Union's General Data Protection Regulation (GDPR) on private company policies on the other side of the world are an example of this type of cross-border influence.

The Internet of things seems like a local concern, on its surface. Cyber-embedded objects have a hard, material presence in the real world. A piece of equipment in a factory or a medical monitoring device in a home are clearly tangible objects, not just information or human communication understood virtually through screens. Yet they are not merely local policy concerns, any more than a social media application that someone accesses in a home is a local policy concern. These local objects and the systems that connect them are a global policy frontier entangled with international security, geopolitical conflict, and human rights.[30] Because they connect to the Internet, there is always the possibility of someone reaching across borders to access a cyber-physical device. In some cases, the intermediating networks and technologies are different from, although they build on, the technologies supporting content-centric systems. But they also rely on the same core networks, interconnection points, and systems of routing.

If distributed infrastructure points of control shape, constrain, and enable the flow of communications (email, social media, messaging) and content (e.g., Twitter, Netflix, Reddit), infrastructure connected to the physical world (bodies, objects, medical devices, industrial control systems) to a much greater extent is able to exert economic and political effects. Global control struggles

materialize at boundary points of "transduction" via sensors and actuators. Direct connections between the digital world and the physical world now proliferate. Door locks are digitally connected and can be operated without being touched by a human hand. Medical devices inside the body can convert biological measurements into digital signals transmitted over a network.

For these systems, the essence of control capability is transduction, the conversion of signals and energy forms from the physical world into the digital world, and the inverse. Examples of this conversion include electrical signals converted into pressure, or temperature in the real world converted to an electrical signal. Digital networks monitor and control real-world, material objects. Sensors capture a reading (e.g., temperature, pressure, movement, sound waves) in the real world and convert them to digital signals for transmission over a network. Actuators take the instructions from a digital signal and convert this form of energy and act on the physical world, such as causing rotary motion or a chemical reaction.

A recalibration of technology policy debates is necessary to account for the rising potential and implications of transduction. One distinction theorists have made between cyber war and "real-world war" is that cyber conflict does not result in human death. This distinction collapses as an increasing number of critical real-world systems become cyber embedded. For example, while autonomous vehicles will save lives because so many accidents arise from human error, digital networks control these vehicles, and hackers anywhere in the world can potentially sabotage or disrupt them, potentially resulting in human death.

This direct, connective manipulation of the physical world from anywhere in the world via a digital network is a powerful form of control, enhancing human life and industrial efficiency but also creating terrifying possibilities for disruption, manipulation, surveillance, and conflict—as close as within a body and as far away as industrial control systems located on the other side of the world.

The expansion of cyber into real-world, everyday objects, logistical networks, and industrial systems expands the national security threat base, the types of foreign intelligence possible, and what counts as cyber offense. Cyber is already viewed as the fifth domain of warfare. Catastrophic cyber war is not yet inevitable, but politically motivated cyber conflict is an everyday occurrence ranging from cybersecurity attacks on dissident groups to the Chinese hack of millions of records of U.S. federal government workers. Politically

motivated cyber-physical attacks have already moved into critical infrastructure such as the energy sector.

A critical and novel point of control, and therefore policy concern, is how interventions and attacks in the physical world can then translate into digital manipulation, as opposed to how digital interventions can influence the physical world. The possibility of transductive attacks involving manipulation of physical readings to attack or mislead digital systems completely transforms the object of analysis of cybersecurity, which now has to leave digital networks and data stores and extend into protection from manipulation originating in the physical world.

Policy issues around intermediaries also become more complicated. What counts as intermediation in cyber-physical systems and the institutional and socioeconomic forces that shape this intermediation are more concealed and heterogeneous than traditional communication intermediation. The philosopher Bruno Latour asked in 1994, "Why is it so difficult to measure, with any precision, the mediating role" of technology or what he called "techniques"? "Because the action that we are trying to measure is subject to 'blackboxing'—a process that makes the joint production of actors and artifacts entirely opaque. Daedalus' maze is shrouded in secrecy."[31] As Latour explains, the black box itself also changes the meaning of its context, such as a speed bump shifting from an objective of not striking a neighborhood child to not damaging the suspension of one's own car. A translation occurs. Cyber-physical system intermediation may be a modern recapitulation of the Labyrinth in Greek mythology.

The cyber-physical upheaval is heterogeneous and pervasive. There are many emerging areas of technological innovation in which digital technologies are becoming embedded into the physical world. Chapter 2 examines four of these. The digitization of everyday objects includes consumer Internet of things and connected objects in smart cities. The Internet of self encompasses cyber-physical systems entangled with the body, such as wearable technologies, implantable chips, biometric identification devices, and digital medical monitoring and delivery systems. The industrial Internet of things, sometimes called the "fourth industrial revolution," involves restructurings of industries and labor around cyber-physical systems. Finally, emergent embedded systems include those embedded objects that are born digital, such as robotics, 3D printing, and arguably augmented reality systems. Understanding these heterogeneous

technical architectures, and the technological affordances and characteristics they all share, is necessary for understanding emerging governance debates.

The policy issues that arise in cyber-physical systems create new problems and challenges that are more complicated and arguably more critical than even in traditional communication systems. Part 2 of the book, "The Global Politics of Cyber-Physical Systems," breaks these emerging governance issues into three arenas: privacy, security, and interoperability.

Cyber-physical system privacy concerns encroach into intimate spaces in and around the body and in material spaces of industry, the home and society that were once distinctly bounded from the digital sphere. Chapter 3 addresses this critical area. Privacy problems are also concerns about discrimination, such as using collected data for employment, insurance, and law enforcement decisions. Privacy problems in digital-physical spaces also raise a host of national security concerns. The chapter explains some of the constraints that complicate privacy and recommends a baseline privacy-protection framework to address this extraordinary policy challenge.

Cybersecurity increasingly connects to consumer safety and critical industrial infrastructure, as well as the digital economy and systems of democracy. Chapter 4 explains how the stakes of cyber-physical security have never been higher. From attacks on the energy sector to the attacks on the consumer IoT and democracy, cybersecurity governance is an existential concern in society. Regrettably, security is woefully inadequate. Market incentives privilege rapid product introduction rather than strong security. This chapter suggests baseline recommendations, across all stakeholders, necessary for improving the cyber-physical ecosystem. It also explains how cyber-physical systems complicate and increasingly shape already-difficult global cybersecurity governance questions such as when governments choose to stockpile knowledge of software vulnerabilities for cyber offense, rather than disclose them to secure critical infrastructure.

Chapter 5 examines how technical standardization faces unique challenges. Embedded objects require high security but are also constrained architectures that demand lower energy consumption and restricted processing power. The current state of interoperability is fragmented, heterogeneous, complex, and involving multiple competing standards and an expanding base of standards-setting organizations. Unlike traditional communication systems that require universality, fragmentation by sector might actually have beneficial effects,

such as serving as a de facto security boundary. The chapter explains the evolution of fragmented standards in the IoT space but suggests that open standards and interoperability in the underlying common infrastructure are still vital for accountability, innovation, and stability.

The complicated concerns arising in cyber-physical systems necessitate a reconceptualization of long-held beliefs about Internet freedom. They also call into question dominant approaches, ideologies, and power structures in global Internet governance regimes. Part 3, "Rethinking Internet Freedom and Governance," addresses the cognitive dissonance between how technology is rapidly moving into the physical world and the conceptions of freedom and global governance that remain in the communication governance world.

Decades of cultural and political thought have sought to understand human autonomy and digital rights in the context of the Internet as an online public sphere for communication and access to knowledge. The goal in democratic societies has been to preserve "a free and open Internet," an uncritical concept that has become somewhat of a fetishized ideal. Chapter 6 suggests that all of the various conceptions of Internet freedom have to be challenged in light of technological change. Internet freedom has a long history, but all incarnations center on the transmission and free flow of content, from John Perry Barlow's "A Declaration of the Independence of Cyberspace" and calls for freedom from regulation to the United States Department of State's Internet freedom foreign-policy campaign. Normative frameworks should adjust both to the realities of information control from private ordering and authoritarian power and the rising human rights challenges of cyber-physical systems.

Structural transformations also challenge prevailing Internet governance power structures, imaginaries, and approaches. Provocations for the future of Internet governance are taken up in chapter 7. Policy entanglements with previously distinct spheres—consumer safety, systems of democracy, cryptocurrency, and environmental protection—expand the scope of global Internet governance. Power relations in the multistakeholder governance regime shift as new companies, new standards regimes, and new tensions arise between bordered government regulatory responses and a global cyber-physical architecture. The rising stakes of digital security, such as to consumer safety and national security, challenge some venerable norms of Internet governance. Notions of a free and open Internet, still vitally important, move toward notions of security, stability, and reliability.

Privacy and security have to take primacy as aspirational values as networks shift from digital only to directly embedded in the physical world. Chapter 8 concludes the book with a call for various stakeholders to urgently take serious cyber-physical policy choices and collectively elevate cybersecurity as a generational imperative necessary for human security, economic security, and national security. For example, a long-standing Internet policy tradition, while varying by region, is immunity from liability for information intermediaries. What counts as an intermediary in cyber-physical architectures and how should risk, accountability, and liability be reconceptualized in the high-risk era?

The technological diffusion of the Internet into the material world requires new approaches to technical architecture and governance that not only consider the content-centric protection of the digital economy and the free flow of information but also view infrastructure stability and cybersecurity as a critical human rights issue. The Internet, as a communication network, transformed how people communicate with each other and interact with information. The Internet, as a cyber-physical control system, is transforming how humans interact with the material world. This book is a provocation both to "see" digital infrastructure as it is and to understand and reimagine the politics embedded in this infrastructure. More importantly, it is the hope that this book will be of interest to any citizen concerned about the future of human rights in our digital future, in which offline and online spheres become completely indistinguishable.