Summer 2019 www.uclajolt.com Volume 23, Issue 2

UCLA Journal of Law & Technology

WHO IS IN CHARGE HERE?

THE INTERNET OF THINGS, GOVERNANCE AND THE GLOBAL INTELLECTUAL PROPERTY REGIME

Andrew Rens †

Abstract

No one entity is in charge of the Internet, yet it works. The functioning of the Internet is maintained by an amalgamation of technological architectures, standards (and standards bodies) and task specific institutions, that are referred to as the Internet governance regime. But this mode of organization faces new challenges. Increasingly everyday objects, from cat feeders to traffic lights, are being fitted with sensors and controls and then connected to the Internet. The resulting Internet of Things is beset with problems of security, safety and privacy which demand public policy solutions. Yet the range of potential solutions is constrained by the global intellectual property regime. Development of technical standards is menaced by patent hold up and royalty stacking. Anti-circumvention laws threaten security research and remediation and prohibit owners and users from fixing their own property. The incompatible paradigms of Internet governance and the global intellectual property regime collide on the policy frontier of the Internet of Things.

† BA, LLB, LLM (University of the Witwatersrand), SJD (Duke); Postdoctoral Researcher Internet Governance Lab, American University, Visiting Scholar in the Program on Information Justice and Intellectual Property at Washington College of Law

TABLE OF CONTENTS

Who is in Charge Here? The Internet of Things, Governance and the Global Intellectual Property Regime

Andrew Rens

Introduction

Home hubs that spy on their owners, hackers using home security cameras to threaten families, expensive appliances rendered immediately unworkable at the whim of manufacturers; these are just a few of the new kind of problems encountered with the Internet of Things (IoT). Press reports on the IoT are full of worries about security, privacy, and ownership. But who exactly is in charge of the IoT? The answer is the same as to a question that is no longer asked: who is in charge of the Internet? It has come to be accepted that there is no single authority for the Internet, no-one in charge. But what does this mean for addressing the growing policy challenges of the IoT?

It seems almost anything can be connected to the Internet: 3D printers, cars, traffic lights, and even toasters. This proliferation of Internet enabled devices, the IoT, raises a cloud of complex problems of ownership and control, privacy and surveillance, and ubiquity and network fragility. These problems that demand policy responses are so varied, numerous, and novel that the IoT has been described as a "global policy frontier."[1] National legal systems have regulated many things in the IoT, in some cases for centuries. For example, English and US common law have refused attempts by the former owner of personal property (chattels) to impose conditions on subsequent owners.[2] Tort, property and contract rules have been developed for what have been up until now ordinary objects, without microprocessors or connections to the Internet. But the drafters and interpreters of those laws never imagined that the future generations of the things that they were regulating would one day include computer chips, run software, and be connected to the Internet. It is therefore not surprising that the application of existing laws will produce some unanticipated results, several of which are discussed in Part II.B. However, as cars, cows, and cardiac monitors are connected to the Internet, problems with cars, cows and cardiac monitors become problems for the Internet and thus for Internet governance.

[1] Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 U.C. DAVIS L. REV. 475 (2017).

[2] Molly Shaffer Van Houweling, *The New Servitudes*, 96 GEO. L. J. 885, 906–10 (2007).

The Internet is primarily governed by a concatenation of technologies, protocols, standards, private legal rules, and practices operating across jurisdictional borders, as well as national laws. Standards, protocols and the like emanate from engineering standards organizations, registration bodies, and similar organizations rather than more conventional political actors. This amalgamation is referred to as the Internet governance regime.[3] Most of the theoretical description of Internet governance is derived from regime theory, a paradigm first elaborated in the study of international relations but which has found application in other fields of inquiry. Regime theory was initially used to describe the interactions between nation states through treaties and other international agreements, and the institutions which govern their interactions.[4] One preeminent example of a regime is the global intellectual property regime which is characterized by not only multiple treaties but also by multi-lateral institutions and the enforcement power of the World Trade Organization.[5]

The governance of the IoT exhibits the same super complexity as Internet governance generally, with multiple sites of governance and actors operating across legal borders. Because the IoT has physical effects and enables surveillance, cybercrime, and cyberwar on unprecedented scales, it

[3] There are a number of divergent accounts of Internet governance. I follow the approach taken by Laura DeNardis which is to view Internet governance through a science and technology studies (STS) lens in which technologies, legal instruments and practices are as visible as formal institutional arrangements and international organizations. Discussing how Internet Governance may be theorized DeNardis states:

> The primary task of Internet governance involves the design and administration of the technologies necessary to keep the Internet operational and the enactment of substantive policy around these technologies. This technical architecture includes layer upon layer of systems including Internet technical standards; critical Internet resources such as the binary addresses necessary to access the Internet; the DNS; systems of information intermediation such as search engines and financial transaction networks; and network- level systems such as Internet access, Internet exchange points, and Internet security intermediaries. The following sections suggest five features of global Internet governance...: how arrangements of technical architecture are arrangements of power; the propensity to use Internet governance technologies as a proxy for content control; the privatization of Internet governance; how Internet points of control serve as sites of global conflict over competing values; and the tension between local geopolitics and collective action problems in Internet globalization.

LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE 6–7 (2014). As DeNardis sets out control over technology and privatized institutional arrangements operate in place of formal government control (*Id.* At 11–13.), thus constituting a unique form of international regime.

[4] For a discussion of spread of governance theory see B. Guy Peters, *Governance as Political Theory*, THE OXFORD HANDBOOK OF GOVERNANCE 19–27 (2012).

[5] Laurence Helfer, *Regime Shifting: The TRIPs Agreement and New Dynamics of International Intellectual Property Lawmaking*, 29 YALE JOURNAL OF INTERNATIONAL LAW 1, 6,12,18-23,25-27 (2004).

represents an existential challenge to the current Internet governance regime.[6] How and whether the current flexible Internet regime can adapt to the IoT is constrained by the more rigid global intellectual property regime. The policy space in which solutions to the problems of governing the IoT will be addressed is similarly constrained. However, the constraints on governance of the IoT imposed by the global intellectual property regime at both national and international levels are not widely recognized or appreciated. As discussed in Part III of this article intellectual property problems of the IoT include patent gridlock, weaponized anti-circumvention rules, and trade secrets for algorithms and data. These problems threaten not only the development of the IoT but severely constrain the possibilities for global governance of the IoT. Of course, this is not the first encounter between the intellectual property regime and Internet governance.[7] An earlier encounter resulted in the reconfiguration of Internet governance to accommodate the global intellectual property regime, but the final relationship of these regimes is still unresolved.[8] In the current encounter how will the global intellectual property regime affect the reconstitution of Internet governance demanded by the IoT?

I. Internet Governance and the Internet of Things

A. An Internet of Things

1. Networked Devices

When we think of the Internet we may think mostly of the devices which we use to connect to the Internet, laptops, tablets and phones. But the Internet has always included other things; network servers, modems and printers. More recently the Internet increasingly includes sensors and control devices which are not directly supervised by humans but instead communicate with and respond to other computers. This IoT[9] is not only changing the makeup of the Internet but it challenges the existing arrangements for Internet governance. The term "Internet of Things" was created by Kevin Ashton, at the time an executive at Proctor and Gamble, who began

[6] DeNardis, *supra* note 1, at 477–78, 484–88.

[7] For a sample of the kinds of issues encountered in the past, from the perspective of intellectual property scholars see INTELLECTUAL PROPERTY AND THE REGULATION OF THE INTERNET (Susy Frankel & Daniel Gervais eds., 2017).

[8] DeNardis, *supra* note 3, at 173–98

[9] The Internet of Things is sufficiently novel as to require definition and some description. Yet one is reminded forcibly of the practice in early Internet scholarship of attempting to define and describe the Internet, and how abruptly that practice ceased, whether because one could assume that the audience was intimately familiar with it or because adequate definition and description became impossible if indeed those reasons can be disentangled.

reorganizing supply chains with the use of Radio Frequency Identification tags (RFID).[10] Ashton realized that things would become increasingly easier to monitor.[11] He later articulated the need for the term; "We need an internet for things, a standardized way for computers to understand the real world."[12] A 2016 Organization for Economic Co-operation and Development (OECD) report describes the IoT as "an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world."[13] Less abstractly, the IoT involves embedding both sensors and actuators into objects and then connecting those sensors and devices to the Internet so data flows from the objects and instructions are transmitted to the objects.[14] Neither the data nor the consequent instructions need to involve humans. Instead, both may be managed by software.[15] IoT is as much the remote servers, software, databases, and protocols which enable them all to function together as it is the Internet connected objects themselves.

Connecting everyday devices to the Internet could change manufacturing, transport, agriculture, and domestic life dramatically. Accurate, timely, precise data from the IoT can improve analysis and decisions and accurate, timely, precise control through the IoT can improve efficiency. According to proponents, its potential includes dramatically increasing innovation, easing traffic flow, and even saving megafauna from poachers.[16] The IoT is an important factor in the not yet realized Fourth Industrial Revolution[17] of "just in time" mass customized, and lean manufacturing. But the potential of the IoT has already led to some exaggerated expectations; one expert even claimed: "Every THING in this world will be connected to each other via INTERNET so that we can know anything we want to know."[18] Gartner, a global research firm,

[10] Chana R. Schoenberger, *The Internet of Things*, FORBES (Mar. 18, 2002, 12:00 AM), https://www.forbes.com/global/2002/0318/092.html#33f75a713c3e.
[11] *Id.*
[12] *Id.*
[13] GAËL HERNÁNDEZ, ORG. FOR ECON. CO-OPERATION AND DEV., THE INTERNET OF THINGS: SEIZING THE BENEFITS AND ADDRESSING THE CHALLENGES 5 (2016).
[14] *Id.*
[15] *See generally* William H. Dutton, *The Internet of Things* 8–10 (2013), https://ssrn.com/abstract=2324902 or http://dx.doi.org/10.2139/ssrn; Prasanna Lal Das et al., *Internet of Things: The New Government to Business Platform - a Review of Opportunities, Practices, and Challenges* 25–27 (World Bank Grp., Working Paper No. 120876, 2017).
[16] Sean Gallagher, *We Know You Hate the Internet of Things, but It's Saving Megafauna from Poachers*, ARS TECHNICA (June 6, 2018, 9:00 AM), https://arstechnica.com/information-technology/2018/06/rhino-iot.
[17] Dutton, *supra* note 12, at 4.
[18] S.C. Mukhopadhyay & N.K. Suryadevara, *Internet of Things: Challenges and Opportunities*, *in* INTERNET OF THINGS: CHALLENGES AND OPPORTUNITIES 19, 46–47 (Subhas Chandra Mukhopadhyay ed., 2014).

describes a cycle of expectations and their realization or failure through its hype curve. The curve describes expectations of new technologies as building slowly at first and then rapidly peaking. Unmet expectations lead to disillusionment. It is usually after this has all happened that the technology matures and ultimately becomes productive. Gartner placed the Internet of Things at the top of the curve for emerging technologies in 2014[19], but by 2015 it was shown as past the top of the curve; expectations would continue to fall.[20]

How exaggerated expectations may be is nicely illustrated by the story of the Juicero. The Juicero was the brainchild of Doug Evans, who previously founded a chain of juice restaurants. The device was intended to be a Wifi connected juice press that would squeeze packs of chopped fruit and vegetables to produce fresh juice. A Juicero was able to read a code on the packs to ensure that the contents had not expired and would only squeeze fresh packs that it identified as provided by Juicero. With both juicing and the IoT *en vogue*, along with a complementary products strategy[21], the Juicero proved very attractive to investors, who invested between $120 and $134 million. Introduced to the market in March 2016, the Juicero was initially priced at $699, although the price was later dropped to $350, while the packs of pre-cut fruit and vegetables cost between five and eight dollars.[22] Despite a number of patents[23] and a patent and trade dress complaint against the Froothie Juisir, the Juicero's press and pack system proved less innovative than originally claimed. In April 2017, a Bloomberg article disclosed that the packs could be squeezed by hand faster than with the press and giving nearly as much juice.[24]

A number of investors had not known that the actions of the press, with 400 customized parts, could be so easily replicated by hand. In the wake of the article, investor confidence dropped and the company shut down in September 2017. Connecting the press to the Internet may have

[19] A.R. Guess, *Gartner Reports 'Internet of Things' Tops the Technology Hype Cycle*, DATAVERSITY (Aug. 27, 2014), http://www.dataversity.net/gartner-reports-internet-things-tops-technology-hype-cycle.
[20] Kasey Panetta, *5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018*, SMART WITH GARTNER (Aug. 16, 2018), https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018.
[21] Often referred to as a razor and blades model in reference to the introduction of the safety razor by King Camp Gillette. While this sobriquet is well known, for those unfamiliar with the concept *see* Iman Ahmadi et al., *Time Preferences and the Pricing of Complementary Durables and Consumables*, 34 INTERNATIONAL JOURNAL OF RESEARCH IN MARKETING 813, 814 (2017).
[22] Ashley Carman, *Juicero, Maker of the Doomed $400 Internet-Connected Juicer, is Shutting Down*, THE VERGE, (Sept. 1, 2017, 2:28 PM), https://www.theverge.com/2017/9/1/16243356/juicero-shut-down-lay-off-refund.
[23] A search of the United States Patent and Trademark Office online Database shows Juicero as the applicant for 28 patents including 10 separate patents for a juice pouch, referred to as a cartridge. See online patent search of USPTO patent database made on May 1, 2019 on record held by author.
[24] Ellen Huet & Olivia Zaleski, *Silicon Valley's $400 Juicer May Be Feeling the Squeeze*, BLOOMBERG (Apr. 19, 2017, 2:00 AM), https://www.bloomberg.com/news/features/2017-04-19/silicon-valley-s-400-juicer-may-be-feeling-the-squeeze.

had some marginal benefit for consumers since they would then not have to make the effort to read the expiry date on the packs. But the benefit for the manufacturer was much greater. Not only could it prevent the use of juice packs from competitors, and re-use of juice packs by customers but it would accumulate aggregate market data on which products were consumed and data on the habits of individual consumers and households. This data could then be sold to data brokers who might sell it to health insurance companies, marketers, and even online dating companies. The history of the Juicero shows that there is an ominous appetite for investment in the IoT that will accumulate data about the domestic habits of consumers. It also shows that at least some entrepreneurs and investors naively believe that simply enabling an object to connect to the Internet somehow increases the value of the object.

IoT technologies face graver disadvantages and more intractable challenges than hype and naiveté. A number of factors have led those manufacturing and deploying IoT to make devices which are insecure by design. Many IoT technologies operate with low electrical and limited processing power. Many collect data and transmit it over the open radio frequency spectrum using protocols that were not designed to be secure. Some can affect the health and safety of people but this is not always apparent to the people whose health and safety is affected. Large numbers of things communicate only with other things without direct human supervision. The result is not only that individual objects can be hacked, but that entire systems are vulnerable, raising the threat level from a corporate IT department worry to a national security concern. Other factors create threats to privacy. Many IoT devices are designed to collect large amounts of data but not to allow those subject to collection any power over what is collected or how it is used.

The simple protocols of the Internet have proven very successful at achieving their original purpose; exchange of information. But, the Internet was not designed for situations where that information can remotely stop cars and hearts. The Internet succeeded because of its design as an end-to-end network, or better: a network of networks. Up to this point in history there have been almost no constraints on what could be connected to the Internet, provided that whatever was connected could communicate using the standard protocols. The protocols by which the networks communicate are simple, and therefore robust, allowing the devices connected to the network to deal with information in complex ways, unconstrained by a network that demands too much.[25] This is sometimes articulated as a dumb network with smart devices. The IoT, however, connects dumb devices to the network. One way in which these devices are dumb is that many have low processing power and memory and as a consequence are harder to secure even when an effort is made to secure them. Another is that many lack capacity to interface directly with humans, so it is difficult for those affected by them to tell if they have been

[25] Saltzer, Reed and Clark are generally credited with the first articulation of the end to end network principle. *See End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS IN COMPUT. SYS. 277 (1984), http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf.

compromised. One solution is to try to make the network smarter while another is to require that devices connected to it are smart enough to be secure and stable.

An end-to-end network still has some complexity; it can be configured to respond to threats to the network itself, such as cascading failure and distributed attacks. Security and stability do not militate against end-to-end design, indeed end-to-end encryption would make the Internet more secure. But requiring end-to-end encryption would require major changes to Internet protocols. In the meantime, how can minimum standards of security be required of IoT devices? Connected things that pose the most obvious dangers, such as drones, cars, and cardiac pacemakers[26] are already subject to regimes such as aviation, road, and health law which could impose security requirements. But what of the tens of thousands, and soon hundreds of thousands and millions of simpler things; that are not subject to specific safety regulations, such as security cameras, RFID scanners, gate openers?

Enumerating the challenges does not convey the extent of the change portended by the IoT. To understand this potential change, we should recognize objects connected to the Internet as extreme examples of what philosopher of technology, Albert Borgmann, calls devices.[27] Borgmann distinguishes devices and things. A thing, in Borgmann's terminology, "is inseparable from its context, namely, its world, and from our commerce with the thing and its world, namely, engagement."[28] By contrast:

> [D]evices . . . dissolve the coherent and engaging character of pretechnological world of things. In a device, the relatedness of the world is replaced by a machinery, but the machinery is concealed, and the commodities, which are made available by a device, are enjoyed without the encumbrance or the engagement with a context.[29]

Objects connected to the Internet are devices because they offer instantaneous feedback, ubiquity, and ease[30] but conceal their reliance on unseen infrastructure. It may seem counterintuitive to characterize devices that respond to data from their environment as decontextualized, but an example will illustrate how this is so. A smart thermostat can adjust the temperature in a home according to the presence or absence of its inhabitants. It can be controlled by the user through an app on a smartphone, whether the user is physically present or thousands of miles away. Some can learn from the patterns of human behavior to predict when

[26] The security vulnerabilities of a cardiac device caused the FDA to issue a warning in 2017. *See* U.S. FOOD & DRUG ADMIN., CYBERSECURITY VULNERABILITIES IDENTIFIED IN ST. JUDE MEDICAL'S IMPLANTABLE CARDIAC DEVICES AND MERLIN@HOME TRANSMITTER: FDA SAFETY COMMUNICATION (Jan. 9, 2017), https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm535843.htm.
[27] Albert Borgmann, TECHNOLOGY AND THE CHARACTER OF CONTEMPORARY LIFE: A PHILOSOPHICAL INQUIRY (1984).
[28] *Id.* at 41.
[29] *Id.* at 47.
[30] *Id.* at 41.

inhabitants are likely to return home and adjust the temperature accordingly. Whenever the software is closed source[31] it is beyond the knowledge and thus control of the user how the temperature is adjusted, how the patterns are understood and the predictions made.[32] Also beyond the control of the user is what data is collected by the provider of the smart thermostat and in the US, at least, how that data is used.[33] True, a provider may allow a user to set privacy preferences about how her data is used, but too often the user lacks either technological or legal power to determine the use of data for herself.[34] IoT devices conceal not only their reliance on a hidden infrastructure but how that reliance redistributes power. They are thus devices in the Borgmannian sense, concealing the trade-offs and costs of the apparent convenience provided.

Prior to the IoT, scholars of Internet governance had pointed out a trend towards control of Internet infrastructure as well as control through Internet infrastructure. Laura DeNardis and Francesca Musiani observe:

> [I]n an era in which nation-bound laws regarding content no longer neatly comport with the globally dispersed and decentralized architecture of the global Internet, there is increasing recognition that points of infrastructural control can serve as proxies to regain (or gain) control or manipulate the flow of money, information, and the marketplace of ideas in the digital sphere. We call this the "turn to infrastructure in Internet governance.[35]

The IoT is set to exacerbate the turn to infrastructure in ways which current Internet governance seems ill prepared to meet.

2. Boundary Problems

Despite the explanation of the IoT offered, the term remains rather vague, overlapping with a number of associated modish phrases including smart devices, smart cities, and self-driving cars. The IoT overlaps with these ideas in indefinite ways. I do not pretend to resolve the resulting boundary problems here but a brief review of connected concepts helps to give color to what is meant by the IoT.[36]

Au courant concepts such as Big Data, Artificial Intelligence (AI), and 3D printing are often connected to the IoT in public discussion. Big Data refers to data sets too large for manipulation

[31] For example Nest Thermostats software is closed source, see Nest Thermostat End User License Agreement, https://nest.com/legal/eula, accessed May 6, 2019.
[32] Lidiya Mishchenko, *The Internet of Things: Where Privacy and Copyright Collide*, 33 SANTA CLARA HIGH TECHNOLOGY LAW JOURNAL 90, 90–94 (2016).
[33] *Id.* at 97–98.
[34] *Id.* at 90–108.
[35] Laura DeNardis & Francesca Musiani, *Governance by Infrastructure*, *in* THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE 3–4 (Francesca Musiani et al. eds., 2016).
[36] I follow the convention for discussions of these phenomena in giving examples rather than offering comprehensive definitions.

or analysis without specialized software, often provided through AI.[37] AI stands for artificial intelligence but is, for the time being at least, synonymous with machine learning models[38] in which software is generated in response to patterns in data rather than being written as a set of rules by a human.[39] Big Data and AI create demand for data and offer the possibility for the remote control of devices. Replacement parts for machines, and even complete mechanisms such as guns, can be fabricated using 3D printers,[40] which add material, unlike conventional methods which remove material. Like IoT devices, 3D printers can be operated remotely or autonomously. However, 3D printers are relatively complex and expensive compared to many IoT devices.

The "smart city" buzzword is usually used to refer to the deployment of sensors and actuators linked to a network to control city infrastructure but encompasses a political and rhetorical project.[41] One example of 'smart city' technology is smart street lights that turn on only when activated by a network which detects the approach of a vehicle or pedestrian.[42] Another frequently cited example is smart traffic lights, which gather data on traffic flow to be analyzed by a network that changes the timing of multiple traffic lights to manage the flow better.[43] "The smart city" does not include consumer IoT devices nor the machines of the Fourth Industrial Revolution since these are not components of city infrastructure.

Self-driving cars are autonomous vehicles that rely on an array of sensors and software, derived from machine learning analysis of driving data, to operate without a human driver. They are

[37] According to a World Bank report "[b]ig data is an umbrella term used to describe the constantly increasing flows of data emitted from connected individuals and things, as well as a new generation of approaches being used to deliver insight and value from these data flows." *Big Data Innovation Challenge*, Report (World Bank, Washington, DC 2016) iii.

[38] According to an AI Now report "[a]rtificial intelligence (AI) refers to a constellation of technologies, including machine learning, perception, reasoning, and natural language processing." Kate Crawford & Meredith Whittaker, The AI Now Report, The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term, Jul. 7, 2016 2.

[39] According to Tom Mitchell "[a] computer program is said to learn from experience E with respect to some class of tasks T and performance measure P if its performance at tasks in T, as measured by P, improves with experience E." TOM M. MITCHELL, MACHINE LEARNING 2 (1997).

[40] Marco Fey, *3D Printing and International Security: Risks and Challenges of an Emerging Technology*, PRIF REPORTS 144 (2017).

[41] Esther Keymolen & Astrid Voorwinden, *Can We Negotiate? Trust and the Rule of Law in the Smart City Paradigm*, INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY 1, 6-8,14-15,17-18 (2019)

[42] For example Intelligent and coordinated lighting of a lighting device, Patent No. US9854645B2, (filed Aug. 6, 2015) (issued Dec. 26, 2017)

[43] For example Intelligent traffic light control system, Patent No. US20090167561A1, (filed May 13, 2008) (issued Jul. 2, 2009).

intended to operate in existing road environments without the support of smart city infrastructure. Although there are a number of very well-funded efforts underway,[44] at the time of writing, a safe, fully autonomous vehicle has not been demonstrated. Unlike many of the objects of the IoT, self-driving cars are very expensive and rely on multiple costly sensors and extensive software in the vehicle itself. They are, or at least should be,[45] subject to existing regulatory standards for which vehicles may be used on public roads and what constitutes safe driving.

Sensors that monitor the functioning of the body have become affordable and battery technologies have improved so that personal body monitors, often called wearables, have become affordable for consumers, at least in the global North. These include bracelets that monitor heart rate and motion to report on exercise and sleep.[46] Less popular, but likely to gain popularity over time, are implants, such as Internet connected pacemakers and insulin pumps. Together, these technologies enable the kind of bodily monitoring referred to as the quantified self. Unlike most IoT devices, these are intimately connected to the bodies of people. As a result, many of the unsolved problems of the IoT, such as weak security and control over personal data, are particularly acute for these devices. But, these devices are also subject to specific regulatory systems for medical devices and data.

Smart cities, smart cars, wearables, digital implants, and even 3D printers face many of the same issues as IoT devices. While low power, potentially ubiquitous devices are considered typical of the IoT[47] these related phenomena are not all constrained in the same ways, for example smart cars have much greater processing power and more reliable energy sources than most IoT devices. Each of these phenomena results from one or more related technological changes: cheap, low power sensors; massive increases in data gathering capability; machine learning based data analysis and decision making; and cheaper, low power computer chips. Common to them all is reliance on unseen infrastructure. While consumer devices tend to dominate media reports on the IoT, unseen infrastructure is too often disregarded in policy analysis. The result of these technologies is a network able to gather very different kinds of data on scales that were previously unimaginable. But networks now no longer only gather and process data, they exercise control over physical environments. DeNardis describes this as a shift from an Internet

[44] Efforts by corporations as diverse as Uber, Waymo (owned by Alphabet), Tesla and General Motors have not yet produced self-driving cars. Ben Dickson, *The Predictions Were Wrong: Self-Driving Cars Have a Long Way to Go*, PCMAG, Feb. 11, 2019.

[45] The SELF DRIVE Act would have exempted self-driving cars from existing federal, state and local regulations. *See* SELF DRIVE Act, H.R. 3388, 115th Cong. (2017). As of May 2019, the Bill is currently stalled in the United States Senate. *See* https://www.congress.gov/bill/115th-congress/house-bill/3388 (accessed May 6, 2019).

[46] One example is the Fitbit, see FITBIT, https://www.fitbit.com (last visited Apr. 17, 2019).

[47] Mukhopadhyay & Suryadevara, *supra* note 15, at 1.

which was largely centered around humans communicating media (text, video, and the like) to a network characterized by computers controlling things with material effects; in brief, a change from a communications network to a control network.[48] While this change ostensibly offers greater convenience, it extends the "device" paradigm to an increasing range of human activities. What is concealed is who, or rather what, watches and controls physical environments. How will governance of the Internet, which is increasingly the IoT, take this shift into account?

B. The International Internet Governance Regime

1. Internet Governance

When the Internet of interconnected personal computers began to enable global information exchange, it operated through technical protocols without requiring the kinds of cross border legal arrangements needed for mail and telegrams. The Internet presented a challenge to scholars seeking to understand collective control of public endeavors. While the Internet is very much a public entity, the role of the state is indirect; control is exercised through dynamics not easily parsed as forms of government. Instead, collective control is better understood as governance rather than government. Regime theory, developed originally in the study of international relations, has been the frame for most responses to this conceptual challenge. While regime theory has been shown to have its limitations, it has proven useful in analyzing the ways in which the Internet is governed. Regime theory has also proven useful for describing the ways in which intellectual property laws and associated practices have come to form a global system. A time-honored definition of a regime is provided by Krasner:

> Regimes can be defined as sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations. Principles are beliefs of fact, causation, and rectitude. Norms are standards of behavior defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice.[49]

International regimes are formed by international law, especially, but not exclusively, treaties. They are also formed by international non-governmental organizations, such as the United Nations, and international consensus that emerges through the process of these institutions, even when their pronouncements are not directly enforceable through dispute resolution mechanisms. A typical example of this kind of regime is the global intellectual property system; comprised of

[48] Laura DeNardis, *Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance*, 15 INFORMATION, COMMUNICATION & SOCIETY 720, Laura DeNardis, *Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance*, 15 INFORMATION, COMMUNICATION & SOCIETY 720, 726,733-4 (2012).

[49] Stephen D. Krasner, *Structural Causes and Regime Consequences: Regimes as Intervening Variables*, 36 INT'L ORG. 185, 186 (1982).

treaties such as the Berne Convention,[50] the World Intellectual Property Organization (WIPO), and associated norms and decision making.

The Internet unsettled the assumption that a regime is primarily constituted of formal principles, rules, and procedures. It also unsettled inarticulate assumptions that the actors in international regimes are necessarily states and international intergovernmental organizations. DeNardis and Musiani point out:

> What is interesting about Internet governance is that it transcends traditional government centric mechanisms like national statutes or intergovernmental treaties. Governance is collectively enacted by the design of technology, the policies of private companies, and the administrative functions of new global institutions like ICANN and the Internet Engineering Task Force (IETF), as well as national laws and international agreements. This broad ecosystem of institutions, laws, and private ordering that keeps the Internet's infrastructure operational, as well as the enactment of public policy around this infrastructure, is generally called Internet governance.[51]

The difference between Internet governance and government should not, however, suggest an absence of power or control. "These administrative and coordinating functions have always been instruments of power because of the ever-growing importance of the Internet to global systems of economic trade, social life, and the political sphere."[52] An important sect of actors in the formation, maintenance, and control of the Internet is technical standards bodies, such as the Internet Engineering Task Force[53] and the World Wide Web Consortium (W3C).[54] Many of these were not the kind of actors that political science was accustomed to dealing with; lawyers were equally uneasy with actors that were often not legal persons at all.[55] Law does play some role in Internet governance, but even then in forms to which regime theory has not paid much attention: for example, the contracts between Internet Corporation for Assigned Names and Numbers (ICANN) and controllers of top level domains (TLDs) are a form of law, but are a private agreement rather than an international treaty. Even if the actors and forms were unfamiliar to many scholars, the Internet demanded a theoretical explanation: "While the Internet

[50] Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, as revised at Paris, France, July 24, 1971, 102 Stat. 2853, 331 U.N.T.S. 217.

[51] Laura DeNardis & Francesca Musiani, *Governance By Infrastructure*, *in* THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE 4 (Francesca Musiani et al. eds., 2016).

[52] *Id*.

[53] INTERNET ENGINEERING TASK FORCE (IETF), https://www.ietf.org/a (last visited Apr. 12, 2019).

[54] WORLD WIDE WEB CONSORTIUM, https://www.w3.org (last visited Apr. 10, 2019).

[55] While some standards bodies do make use of various for profit or non-profit corporate structures, in my view it is a category mistake to treat these, rather than the deliberating collectives that set standards, as the actors of Internet governance since their power is exercised through the making of standards which does not require separate legal existence.

has become a very stable global communication platform, the fact that it 'just works' is no accident."[56]

DeNardis proposes that any examination of Internet governance must take place within at least four parameters. These can be paraphrased as: (1) Internet governance must distinguish Internet governance from broader descriptions of how people use the Internet; (2) it must focus on the technologies that connect the "network of networks" of the Internet, rather than digital information and communications technologies generally; (3) examination should take into account not only institutions, but also technologies, private actors, and laws (national and international); and (4) while technologies and policies that enable the Internet to function so that information flows are important to Internet governance, so are efforts to limit information or engage in surveillance.[57] Insisting that Internet governance is confined to what makes the Internet the Internet, rather than what the Internet enables or changes, brings useful focus to a complicated and rapidly changing phenomenon. It also sets up a tension between the focus on technology standards, functional bodies, and the broader dynamics which affect these, which shapes policy debates about the Internet.[58] This tension may be endogenous to an ecosystem that includes not only international intergovernmental organizations, regional and national governments, standards bodies, but also private corporations operating through public-private partnerships and provisional, limited processes created under the pressure of immediate challenges.[59]

2. Law and the Internet

If Internet governance singularly and strikingly rejects law as its primary mode, what has that meant for interactions of law and the Internet?

"Government policy approaches toward the Internet should therefore start from two basic principles: avoid unnecessary regulation, and question the applicability of traditional rules."[60] This statement comes not from a cyberlibertarian, nor from a whiz kid entrepreneur whose start-up is disrupting an industry. Instead, it comes from Kevin Werbach, who at the time was a lawyer working for the Federal Communications Commission, albeit disclaimed as not representing the views of the agency. Written in 1997, it is representative of the dominant

[56] Derrick L. Cogburn, *The Multiple Logics of Post-Snowden Restructuring of Internet Governance*, *in* THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE 25, 26 (Francesca Musiani et al. eds., 2016).
[57] DeNardis & Musiani, *supra* note 45, at 6.
[58] *See* Cogburn, *supra* note 53, at 30.
[59] Nanette S. Levinson & Meryem Marzouki, *International Organizations and Global Internet Governance*, *in* THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE 47, 51–52 (Francesca Musiani et al. eds., 2016).
[60] Kevin Werbach, *Digital Tornado: The Internet and Telecommunications Policy*, at ii (Fed. Commc'n, Office of Plans and Policy Working Paper No. 29, 1997).

framing of initial encounters of law and the Internet. According to this approach, while some regulation might be necessary to enable Internet transactions[61] and to ensure competitive provisions of underlying telecommunications infrastructure,[62] new laws should not be made for the Internet and, where existing law is to be applied, that application should not be permitted to restrain innovation. There are a number of competing narratives of this first encounter between law and the Internet. Because these are discussed extensively by others, my purpose is just to make key distinctions.

According to one viewpoint, innovation is fast, while law is slow. In some versions of this viewpoint, law must try to catch up with innovation, but while law can make progress, it will never quite catch up with innovation but will instead be locked in pursuit. This viewpoint may include a warning that law should not regulate innovation too aggressively since it is bound to misstep, sometimes harming innovation, sometimes only exposing its clumsiness. In another version of the law-lagging-technology viewpoint, law lags hopelessly far behind innovation, so far that it is pointless to try to regulate innovation. This latter position has often been coupled with the idea that the Internet is somehow immune to regulation due to its design. John Gilmore articulated this when he stated that the Internet "interprets censorship as damage and routes around it."[63] The use of 'censorship' here was taken to be any state attempts to control the distribution of information, not just for political purposes but efforts by courts to prevent information being shared because it was held to be defamatory, infringe copyright, or similar civil claims.

Despite these ideas, as the subsequent history of the Internet makes clear, particularly in China, Iran and Zimbabwe, states can exercise some power over the Internet, if only to sequester portions of the network and disable key functions in the sequestered network. In the early days of the Internet, Gilmore's claim was bolstered by the special low regulation approach championed by Werbach. However, the regulators that followed that approach did not

[61] Werbach states:

> Those who oppose 'regulation of the Internet,' generally do not wish to make the Internet a zone in which all government authority, such as prohibitions on theft and fraud, or guarantees of property rights, cease to exist. Rather, the debate is about whether new legal constructs are needed to address Internet-based transactions, and whether existing constructs meant for different situations should be applied to the Internet. In other words, would a particular type of service, offered by a particular type of company, be subject to particular requirements and prohibitions? The Commission can and should greatly limit the extent to which its actions interfere with the functioning of the Internet services market.

Id. at 29.

[62] *Id.* at 82–84.

[63] Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME (Dec. 6, 1993), http://content.time.com/time/magazine/article/0,9171,979768,00.html.

necessarily think that the Internet could not be regulated, but rather that regulation should be tempered lest it shut down innovation. This was the general approach adopted by the United States, where the Internet originated. This cannot be characterized as laissez-faire since it required legal and policy action to insulate Internet service providers from the application of existing legal rules. This is demonstrated by the changes to Internet service provider liability. A few early cases suggested that Internet service providers might be liable for the information which they transmitted or hosted. In a defamation case, *Cubby v. CompuServe*, a hosting service was treated as a distributor rather than publisher of news.[64] The hosting service was not liable for publishing defamatory material, because it did not know nor did it have reason to know that statements it was hosting were allegedly defamatory. Another court, in *Stratton Oakmont v. Prodigy*, noted in dicta that hosts such as bulletin boards should be treated the same as bookstores and libraries, meaning they would be liable only if they knew or had reason to know that a statement was defamatory.[65] However, if there was any attempt to permit some information and not other information, for example to provide a "family friendly" service, then liability could be imposed even if the control was not set up to prevent defamatory or otherwise unlawful material. To prevent the extension of common law liability, service providers were given unqualified immunity through federal legislation which stipulated that, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[66]

This history may seem to bolster the theory that law lags behind technology. Yet explicit legal provisions which exempt quotidian activities conducted through a new technology from existing legal rules suggests a different understanding. In this understanding, law co-constructs the meaning and functioning of technology in society, in this case through affording a privileged status to an innovation.

Since the Internet was primarily a means of communicating information to users, the legal issues were informational, including: freedom of expression, defamation, contracts, copyright and privacy. It might seem counter-intuitive to categorize contracts as informational, but since a contract is at least in theory an offer and acceptance, it is in essence information. Legal responses in the categories of speech, defamation, contracts and privacy demonstrate the protected innovation zone approach. As demonstrated above, service providers were exempt from liability for defamation. Courts, and widespread practice, enabled contracts of adherence in which users cannot negotiate but are bound by the mere act of using, reading or clicking an image of a button on a webpage to indicate consent. For privacy, it was required only that persons be taken to have consented to give up their private information through contracts of adherence. Central to the evasion of constraining regulation has been the "logic of expressive

[64] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).
[65] Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *4–5 (N.Y.S.2d May 24, 1995).
[66] 47 U.S.C. § 230(c)(1) (2018).

immunity,"[67] or in other words, of First Amendment protection for speech. Not all jurisdictions have been as chary of regulating speech as the United States.

There is a significant single exception to the protected innovation zone approach. Copyright and trademark are informational, and disputes about both were the bulk of early cases and writing on Internet legal issues. The same federal law that exempted service providers from liability for speech stated, "[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property."[68] The exceptional treatment of intellectual property in Internet governance is discussed in Part III of this paper. At this point, simply note that although some attempt was made to prevent copyright from weighing down the newly weightless sharing of information enabled by the Internet, it has proven largely unsuccessful. Internet service providers were offered a heavily qualified limitation of liability but only in exchange for taking down allegedly infringing content. Intellectual property became the law applied most strongly to the Internet in an as-yet-unresolved power struggle between intermediaries now referred to as platforms and intermediaries invested in restricting information flow through copyright,[69] both in the United States and internationally.

If law would not usually control the flow of information through the Internet, that did not mean that control would not be exercised. Instead, the legal innovations freeing Internet service providers laid bare an existing reality: the extent to which the infrastructure of the Internet and the private actors who run it have become increasingly important to the regulation of information.[70] At the time, the freedom from regulation enjoyed by private actors which controlled Internet infrastructure was portrayed as amounting to the freedom of the Internet. But increased power for a few private actors does not mean increased freedom for everyone. Freedom from direct government control raises problems for democracy and the rule of law. When private actors are able to limit freedom of expression, this gives them inordinate power in democracies in which citizens need to be informed about political alternatives and people need to be able to express themselves.

The global Internet governance regime, which includes but does not operate primarily through law, was coupled with national regimes that explicitly used law to limit the role of law for the Internet. While this was most demonstrably the case in the United States, many other jurisdictions followed similar patterns. For example, South Africa passed Internet-specific legislation which gave service providers qualified exemption from liability and punted on privacy regulation.[71] Subsequently, some jurisdictions have imposed national law on Internet

[67] Julie E. Cohen, *Law for the Platform Economy*, 51 UC DAVIS LAW REVIEW 133, 167–78 (2017).
[68] 47 U.S.C. § 230(e)(2) (2018).
[69] *See* Cohen, *supra* note 64, at 171–73.
[70] DeNardis, *supra* note 45, at 735.
[71] *See* Andrew Rens, *Telkom SA Limited v Xsinet (Pty) Ltd*, 120 S. AFR. L.J. 749 (2003).

communications. But this is often peculiar to the jurisdiction. While some jurisdictions will censor political speech, they have done little to prevent the accumulation of private information by corporations. At least some kinds of information flow seem valued in each jurisdiction, and are thus exempt from regulation that would otherwise apply. But states are also economically reliant on the flow of information through the Internet. The consequence is that generally, the power of nation states to easily control the flow of information has eroded. States began to rely increasingly on private actors for effective law enforcement but also surveillance.[72] Private actors provided Internet infrastructure because it suited them and enabled them to pursue profit. Increasingly, profit has been obtained through advertising, and the more information on users a private company can accumulate, the more precisely it can target advertising and the greater its ability to obtain advertising revenue. A few corporations came to play an outsize role in providing the infrastructure of the Internet, and in pursuit of profit, built an infrastructure of surveillance. Some states proved better able to co-opt the infrastructure-controlled private Internet actors for their own ends than others. Indirect governance became a competitive advantage for a few states, while the inability to co-opt private surveillance infrastructure became a disadvantage for others.[73]

States have thus often chosen to make use of the technologically--based power of a few corporations. These powerful corporations, including Google, Apple and Facebook, are increasingly referred to as platforms. Julie Cohen points out that the power achieved by platforms has been as much the result of entrepreneurial legal strategy and regulatory arbitrage as the architecture of the platform.

> Powerful economic interests have always sought to reshape jurisdictional, procedural, and methodological rules to their advantage. Legal scholars who study judicial and regulatory processes have shown that institutional design responds over time to the interventions of powerful actors . . . . Well-resourced repeat players also work to craft compelling narratives about the structure of legal institutions, pursuing a species of "deep" capture that operates at the level of ideology. Both projects become easier when the ground is shifting.[74]

As the Internet has grown, there has been a greater willingness to impose national or regional law, even when it burdens the communication of information via the Internet, and even by wealthier democracies such as those in Europe. One of the most striking examples of this change is the European Union General Data Protection Regulation (GDPR).[75] The GDPR gives a person whose personal data is held by someone else certain rights over that data; it also

[72] Tatevik Sargsyan, *The Turn to Infrastructure in Privacy Governance*, *in* THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE 189, 189 (Francesca Musiani et al. eds., 2016).
[73] *Id.* at 190–91.
[74] Cohen, *supra* note 64, at 176.
[75] Council Regulation 2016/679, 2016 O.J. (L 119) 1.

imposes obligations including technical security obligations on the holder of the data[76]. But this tightening of Internet regulation is taking place at a national and regional level, rather than internationally. Despite the increased interest in privacy regulation, there is no strong international legal regime that controls the flow of information on the Internet except the global intellectual property regime. At the time of this writing there is not even a candidate. Instead, there is an increased concentration of power over the choke-points of the Internet by private actors.[77]

3. IoT Challenges to the Internet Governance Regime

a) Policy Problems

The interface of the Internet and legal regulation is already complex and changing. Adding the myriad of challenges of the IoT to this interface will only increase the complexity and speed of change. A report to the European Commission in 2013 identified a number of areas of policy concerns: personal data and privacy, security and safety (including the security of critical IoT supported infrastructure), ethical issues such as the ability of users to opt out of automated systems, and interoperability specifically through the need for a global scheme for object identifiers.[78] There was no consensus amongst participants in the public consultation that informed the report whether existing Internet governance structures were adequate to deal with these concerns, nor where regulation is needed.[79] There was general agreement that standards would play an important role in governance of the Internet. An overlapping set of concerns is suggested by Laura DeNardis and Mark Raymond, who organize public interest issues in the following categories: critical Internet resource constraints (such as Internet Protocol addresses), privacy complications, human security, international security, and global competition tensions.[80] In addition to these issues, there are the environmental impacts and a more impalpable concern about the psychological impact of the loss of control over the everyday objects with which we interact.

Current technical configurations of IoT devices underlie the shape of these challenges. A significant subset of devices do not have large power supplies; this affects the rate of processing

[76] Article 6, *id.*

[77] This is elaborated at length by Laura DeNardis as she considers how control over the Internet is exercised by private actors including through technical standards, the role of domain name resolution services, Internet service providers and technologies such as automated deep packet inspection. DeNardis, *supra* note 3.

[78] *See*, EUR. COMM'N DIRECTORATE-GEN. FOR COMMC'NS NETWORKS, CONTENT AND TECH., *Report on the Public Consultation on IoT Governance* (Jan. 16, 2013), ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1746.

[79] *Id.* at 12–14.

[80] DeNardis & Raymond, *supra* note 1, at 478.

in which they can engage and thus the security measures possible. Similarly, a significant subset of IoT devices have far less processing capacity than desktops, laptops and phones. These IoT devices are designed with less capacity because their designers perceive it as unnecessary, or because low power would limit processing in any event, or simply to keep prices down. As with electrical power, low processing capacity reduces available security measures.[81] IoT devices which connect to networks through Wifi and Bluetooth protocols are as vulnerable as those protocols. For example, although Bluetooth was first introduced in 1994, in 2018 a vulnerability in the Bluetooth security protocol was discovered by security researchers.[82] The protocol was subsequently amended to address the vulnerability. But it is not just the technical aspects of the IoT which are different from the Internet for which Internet governance was initially developed, it is also their location. IoT devices such as video and audio recording devices in homes collect masses of intimate data about the domestic lives of their subjects, as do wearables and digital implants. Some IoT devices, such as security cameras, collect data about humans without them being aware that they are being surveilled. But even if they knew they were being surveilled, there is no practical way to refuse consent, and it is not just webcams which are concealed.[83] IoT devices with which people interact tend to follow the tendency Borgmann identified. They conceal the machinery and connections which enable their operation and instead present themselves as "commodities" which apparently unproblematically meet human desires.[84] If devices with which humans interact tend to conceal their machinery, the burgeoning number of IoT devices that interact only with computers are even more easily forgotten.

Foremost of the policy challenges of the IoT is security. While privacy often receives more public attention, without a secure Internet of Things, privacy is impossible. A number of high-profile breaches, of which the Mirai botnet received greatest public attention, indicate not only that the IoT is plagued by security issues, but also that in many cases IoT networks and constituent devices are not secure by design.[85] How to secure the IoT is a technological challenge. But who is responsible for securing IoT devices and networks is a policy question. Associated questions are what the standard of security should be, who will ascertain what standard is required, and what will the consequences be when the standard is not met. But in

[81] *See* Yuchen Yang et al., *A Survey on Security and Privacy Issues in Internet-of-Things,* 4 IEEE INTERNET OF THINGS J. 1250, 1252 (2017).

[82] *Bluetooth Implementations May Not Sufficiently Validate Elliptic Curve Parameters During Diffie-Hellman Key Exchange*, CARNEGIE MELLON UNIV. SOFTWARE ENG'G INST. (Jul. 23, 2018), https://www.kb.cert.org/vuls/id/304725.

[83] For a discussion of the unavoidability of this and its implications for privacy and personal data regulation, see Sarah Johanna Eskens, *Profiling the European Consumer in the Internet of Things*, 48–49 (Feb. 29, 2016) (unpublished Master of Information Law thesis, University of Amsterdam Instituut voor Informatierecht).

[84] BORGMANN, *supra* note 24, at 47.

[85] *See* Yang et al., *supra* note 78, at 1256.

many cases, it is evident that manufacturers are not taking even the most elementary precautions. The makers of Cloud Pets, Bluetooth-connected cuddly toys which allow parents and others to push audio recordings to the toy, exposed the security information of 800,000 users, including passwords online, without any security.[86] The Bluetooth connection on Cloud Pets could also be trivially hacked to turn the toy into a surveillance device.[87] IoT security issues are not just a matter for individuals who might have their privacy infringed or experience a malfunctioning device; compromised IoT devices can also be used to unlawfully surveil people, and in many cases, to cause physical harm. They can also be commandeered to assist in attacks on other network nodes such as Distributed Denial of Service attacks (DDOS) on network servers. If a large number of IoT devices in physical proximity are compromised, they could be used for a large physical attack, for example knocking out a power grid or shutting down a traffic control system. IoT security issues are at the overlap of multiple policy areas: consumer protection, criminal law, and national security.

IoT devices that have been compromised can be used to violate the privacy of people; privacy is reliant on and entangled with security. This problem is not unique to the IoT: laptops and phones which include cameras and microphones have been targeted to enable remote surveillance. But mass collection of personal data about people does not only take place as the result of hacking, it is the raison d'être of many IoT devices. Home hubs and digital assistants constantly monitor sound in their environments in order to respond to key words in their environments. Personal data is not gathered or used discretely by IoT devices, instead, it is integrated into functionality. For example, one proposal for a "smart shop" would laudably reduce energy consumption, but only through tracking identified clients and staff through the shop and adjusting lighting and temperature accordingly.[88] Unlike laptops and smart phones in which cameras and microphones must be deliberately activated, in many IoT devices these may always be on as is the Amazon Echo[89] or turn on automatically without awareness of the people being surveilled. People who have motion sensitive webcams in their homes have found that the cameras filmed them when they were naked and unaware of being filmed and uploaded the video to remote online servers.[90] Owners and users of the devices may not even be aware of the presence of sensors; Nest

[86] Laura Hautala, *Smart Toy Flaws Make Hacking Kids' Info Child's Play*, CNET (Feb. 28, 2017, 2:49 PM), https://www.cnet.com/news/cloudpets-iot-smart-toy-flaws-hacking-kids-info-children-cybersecurity.

[87] *See* Paul Stone, *Hacking Unicorns with Web Bluetooth*, CONTEXT (Feb. 28, 2017), https://www.contextis.com/en/blog/hacking-unicorns-web-bluetooth.

[88] Iván Corredor Pérez & Ana M. Bernardos Barbolla, *Exploring Major Architectural Aspects of the Web of Things, in* INTERNET OF THINGS: CHALLENGES AND OPPORTUNITIES 19, 46–47 (Subhas Chandra Mukhopadhyay ed., 2014).

[89] IOT.DO, https://iot.do/devices/amazon-echo (last visited April 3, 2019).

[90] Kashmir Hill & Surya Mattu, *The House That Spied on Me*, GIZMODO (Feb. 7, 2018), https://gizmodo.com/the-house-that-spied-on-me-1822429852.

thermostats sold by Google include microphones that were kept secret from customers for years.[91] Many 'smart' devices communicate not only with their manufactures or providers, but also with third parties, even if the customer does not sign or have an account with the third party.[92] Manufacturers and service providers have tended to disregard the privacy concerns of users of IoT devices. In 2019 alone, it has been revealed that Amazon permitted employees to access video feeds from Ring cameras even when it was not necessary for them to do their jobs.[93]

Because IoT devices enable gathering of data, they are increasingly targets of law enforcement efforts to obtain data.[94] Public authorities have a number of conflicting interests. They have an interest in IoT devices being secure to prevent both individual and larger, even national attacks. They have an interest in preventing the use of IoT devices for surveillance since this capability can be abused by adversaries. At the same time, they have a conflicting interest in weakening IoT security so that they can use the IoT for surveillance themselves. How laws of evidence, which differ from jurisdiction to jurisdiction, should treat the data gathered by IoT devices, and held by manufacturers, services providers and data brokers is far from clear. For example, with respect to United States law, Andrew Ferguson asks, "is the data trail from an implanted 'smart' heart monitor protected as part of the 'person' as understood in the Fourth Amendment?"[95]

Once corporations create a surveillance architecture it is not only corporations and the state that seek to make use of it. IoT devices have been demonstrated to be vulnerable to hacking. For example, strangers have taken control of baby monitors, listening to and speaking to infants.[96] Motives for strangers taking over corporate surveillance mechanisms may be criminal, mischief making or voyeurism. But it is not only strangers who use IoT devices to surveil and in some cases harass. Abusive partners and former partners sometimes take control of IoT devices to

[91] Zac Whittaker, *Google says Nest's secret microphone was 'never intended to be a secret'*, TECHCRUNCH (Feb. 20, 2019), http://social.techcrunch.com/2019/02/20/nest-secret-microphone.
[92] Nick Feamster, *Announcing IoT Inspector: Studying Smart Home IoT Device Behavior*, FREEDOM TO TINKER (Apr. 23, 2018), https://freedom-to-tinker.com/2018/04/23/announcing-iot-inspector-a-tool-to-study-smart-home-iot-device-behavior.
[93] Sam Biddle, *For Owners of Amazon's Ring Security Cameras, Strangers May Have Been Watching Too*, THE INTERCEPT (Jan. 10, 2019), https://theintercept.com/2019/01/10/amazon-ring-security-camera.
[94] Andrew G. Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 560–66 (2017).
[95] *Id.* at 550.
[96] Sarah Ensenat, *Smart Baby Monitors: The Modern Nanny or a Home Invader*, 26 CATH. U.J.L. & TECH. 72, 72 (2018).

monitor and assail their victims.[97] While this is a relatively recent phenomenon it is part of larger trend in which digital technologies are weaponized by domestic abusers.[98]

Remote surveillance through the IoT provides peculiar difficulties for legal regulation. It is difficult for someone to prove that she has been subject to surveillance if the surveillance does not require the planting of a device but merely the use of the device of the person being watched and when the record of the surveillance is retained on a remote server, inaccessible to the subject. Simply knowing that someone might be watching is sufficient to change a person's behavior.[99] The subject is the only source of information about her choices. If someone refrains from certain actions because she believes herself to be observed then she will be equally reluctant to admit her intended behavior. But even if she is willing to admit that she was dissuaded from certain actions by the possibility of being seen she cannot provide any other evidence. Despite these difficulties it has been extensively demonstrated that technological surveillance modifies behavior.[100] It is not necessary to prove that a human in fact watched another human through a surveillance architecture to conclude that the architecture itself encroaches on the freedom of its subjects. Instead the IoT together with the accumulation of massive datasets analyzed through AI collapses the distinction between surveillance by a person and surveillance by an automated system since the possibility of human observation is subsumed into the system.

[97] Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (Jun. 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

[98] On the larger trend, see Rahul Chatterjee et al., *The Spyware Used in Intimate Partner Violence*, *in* 2018 IEEE SYMP. ON SECURITY AND PRIVACY 441 (2018).

[99] There is an extensive intellectual pedigree for this concept, from Bentham, 11 JEREMY BENTHAM, *Proposal for A New and Less Expensive Mode for Employing and Reforming Convicts*, *in* THE WORKS OF JEREMY BENTHAM, PUBLISHED UNDER THE SUPERINTENDENCE OF HIS EXECUTOR, JOHN BOWRING 165, 165 (John Borwing ed., 1843), to Foucault, MICHEL FOUCAULT, DISCIPLINE AND PUNISH 195–230 (Alan Sheridan trans., Vintage Books 2d ed. 1995 (1977). While I cannot do justice to the many scholars who have used the concept, James Boyle notably applied it to the Internet, James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997), while Shoshana Zuboff has explained how it applies to our contemporary economy. Shoshana Zuboff, *Big other: surveillance capitalism and the prospects of an information civilization*, 30 J. INFO. TECH. 75 (2015).

[100] Elizabeth Stoycheff et al., *Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects*, 21 NEW MEDIA & SOC'Y 602 (2019); Zuboff supra; Antti Oulasvirta et al., *Long-term Effects of Ubiquitous Surveillance in the Home*, in PROC. OF THE 2012 ACM CONF. ON UBIQUITOUS COMPUTING 41 (2012); Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. Q. 296 (2016); Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L. J. 117 (2016).

Technical characteristics of many IoT devices render the network fragile. Software updates can, and too often do, interact with other software to create unexpected results, leading to the malfunction or inoperability of computers and what they control. A simple update to widely used software can inadvertently damage a large number of devices, which affects not just those devices, but also the network. Similarly, problems with network traffic can cause an entire network to become dysfunctional. Even when malfunction is unintended, it renders the underlying physical infrastructure more vulnerable than previously unconnected infrastructure.

Closely connected to network fragility is the concept of safety. The U.S. Consumer Product Safety Commission warns that connecting types of devices previously not connected can introduce or increase the danger of consumers being burned, shocked, tripped or exposed to dangerous chemicals. Reliance on a connection to the Internet or on software updates results in "hazardization" which the Commission describes as "the situation created when a product that was safe when obtained by a consumer but which, when connected to a network, becomes hazardous through malicious, incorrect, or careless changes to operational code."[101]

One consequence of the networked fragility of the IoT is the threat of widespread harm, whether physical or otherwise, which may not be attributable to a particular act, or actor. Legal systems have developed rules, through tort or delict to assign liability for harms to individuals and their interests. Some legal systems enable individuals to act collectively to hold actors responsible for harms suffered by them as a group or class. But legal systems tend to avoid what Judge Cardozo famously characterized as "liability in an indeterminate amount for an indeterminate time to an indeterminate class."[102] Diffuse harms may however still be harms with negative effects on populations, polities and economies. Even when a harm is discrete and a victim can be identified, attributing liability for harm caused by the IoT is complicated. Alan Butler asks whether a manufacturer of an IoT device which is compromised should be liable to the user.[103] While law would attribute liability to the hacker, there is little chance that those who suffered loss could recover damages from difficult to identify actors who may be operating from a faraway jurisdiction. Courts have tended to constrain recovery for "economic loss."[104] Another question is whether the acts of a third party such as a hacker would be regarded as the "proximate cause" of the harm, thus absolving the manufacturer. Yet another question is which standard of liability should be applied; should the manufacturer be held strictly liable or negligent?[105] If the latter, then how will courts determine what security standard is required? A device may have been designed and made to the highest existing standard but rapidly become

[101] The Internet of Things and Consumer Product Hazards, 83 Fed. Reg. 13,122, 13,124 (Mar. 27, 2018).
[102] Ultramares Corp. v. Touche, 255 N.Y. 170, 179 (1931).
[103] Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. MICH. J.L. REFORM 913 (2017).
[104] *Id.* at 919–22.
[105] *Id.* at 916–17, 926.

vulnerable.[106] Is there a duty by a manufacturer that requires a continuous effort to secure a device? If manufacturers should be held liable for damage due to negligence and the actions of others, then should manufacturers be exempt for damage which they cause deliberately?[107]

Some manufacturers deliberately disable IoT devices. SoftComplex, maker of a garage opener controlled from a smartphone, disabled the unit of a customer who posted a critical review of the product.[108] C.A.G. Acceptance auto-finance company remotely disables vehicles of purchasers who have missed a payment, one such incident occurred when a mother was taking her child to hospital.[109] In other instances, sellers have simply permanently terminated support for a product, effectively disabling it. Remote disabling, termed 'bricking' may be due to the failure of a start-up (as with smart light bulb connector Emberlight),[110] but often is a decision by a highly capitalized corporation to simply discontinue support as with the LogiTech Harmony home hub[111] and the Alphabet Revolv.[112] That doesn't mean that the customer can continue operating the device but without software updates, support or warranty, it means that the device stops working altogether. It is useful only as a weight or lump of material, hence the term bricking. Built in obsolescence or planned obsolescence has been used by manufacturers since the 1920's at least. By designing their products so that they will only last a set period so that purchasers

[106] *Id.* at 928–30.
[107] Rebecca Crootof, *Introducing the Internet of Torts*, LAW AND POLITICAL ECONOMY (Jul. 16, 2018), https://lpeblog.org/2018/07/16/introducing-the-internet-of-torts.
[108] Sean Gallagher, *IoT garage door opener maker bricks customer's product after bad review*, ARS TECHNICA (Apr. 4, 2017), https://arstechnica.com.
[109] Michael Corkery & Jessica Silver-Greenberg, *Miss a Payment? Good Luck Moving That Car*, N.Y. TIMES DEALBOOK (Sep. 24, 2014), https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car.
[110] Chris Davies, *Emberlight joins IoT dead pool as its smart lighting goes dark*, SLASHGEAR (Nov. 17, 2017), https://www.slashgear.com/emberlight-joins-iot-dead-pool-as-its-smart-lighting-goes-dark-17508473.
[111] Logitech sold a device called the Harmony Link which, in conjunction with an app on a mobile phone, allowed a customer to remotely control tvs and sound systems. When Logitech abruptly announced in November 2017 that Harmony Link devices would cease to operate from March 18, 2018, without offering an explanation, purchasers were extremely unhappy with the company. Only after negative press coverage did Logitech admit that an internal decision not to renew an encryption certificate was the reason why the devices would cease to operate. Valentina Palladino, *Logitech to shut down "service and support" for Harmony Link devices in 2018 [Update]*, ARS TECHNICA, (Nov. 8, 2017), https://arstechnica.com.
[112] Alphabet, Google's parent company acquired Nest which in turn acquired Revolv which had sold an expensive home hub popular with IoT technology early adopters. On March 1, 2016, the Revlov website abruptly announced that the $300 hub would cease to operate on May 15, 2016. Alex Hern, *Revolv devices bricked as Google's Nest shuts down smart home company*, THE GUARDIAN (Apr. 5, 2016), https://www.theguardian.com/technology/2016/apr/05/revolv-devices-bricked-google-nest-smart-home.

must replace them manufacturers have increased demand for their products.[113] The IoT is marked by a new development: remote control obsolescence. With planned obsolescence, the manufacturer planned how long an item would be useful. A purchaser could hope to predict the useful life of her purchase. But with remote controlled obsolescence, whatever the purchaser plans at the time of purchase is irrelevant since the device can be rendered obsolete at the caprice of the manufacturer or its successor.

Remote controlled obsolescence is just one feature of a more general phenomenon: the erosion of ownership. Rights in property have traditionally empowered the owner to sell or gift, modify or destroy a thing she owns; however two developments are eroding ownership. Firstly, the reliance of devices on software and networked-based services to continue to function makes them subject to control of software and networked service providers. Secondly, contracts, specifically 'End User License Agreements' (EULA's) which incorporate software licenses routinely purport to restrict re-sale and repair of things. The kinds of restrictions over personal property imposed by these agreements have historically not been permitted in US common law.[114] In South Africa, a court required the reconnection of a network service that had been unilaterally disconnected by the network operator. The court regarded the network operators actions as taking the law into its own hands which impaired an owner's use of property.[115] But courts, at least in the United States, have tended to uphold EULA's when they involve software.[116] IoT contracts deal with both things and their connectivity; a hybrid between goods, services and software which courts find difficult to parse.[117] The result of this is a trend that Aaron Perzanowski and Jason Schultz term 'the end of ownership'[118] and Joshua Fairfield calls the 'new digital serfdom.'[119]

Tort, property, and contract are long established legal regimes which courts will apply to the IoT. At the time of the Internet's first rapid spread, and the construction of global Internet governance, it was primarily a means of communicating information. However, the IoT is part of a shift in which the Internet is no longer primarily focused on information sent deliberately by humans. Instead, video, audio and other sensors that gather physical data impose on the bodies of people, while Internet connected things control access to buildings, change temperatures, and determine traffic flows. Although they are well-established, tort, property and contract assume

113 Jeremy Bulow, *An Economic Theory of Planned Obsolescence*, 101 Q.J. ECON. 729 (1986).
114 Shaffer Van Houweling, *supra* note 2.; Christina Mulligan, *Personal Property Servitudes on the Internet of Things*, 50 GA. L. REV. 1121, 1123 (2016).
115 Rens, *supra* note 68, at 754–55.
116 Mulligan, *supra* note 111, at 1123.
117 Stacey-Ann Elvy, *Hybrid Transactions and the Internet of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77, 79–80 (2017).
118 AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY (2016).
119 JOSHUA A.T. FAIRFIELD, OWNED: PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM (2017).

that things function in certain ways, assumptions which no longer hold true for the IoT. Disputes about tort, property and contract are decided in venues remote from contemporary Internet governance. But these legal regimes will increasingly intersect with global Internet governance issues because IoT devices connect to the Internet using protocols, standards and technologies which are the central concerns of Internet governance. While it is not necessary for global Internet governance to provide universal solutions for all of these problems, the issues and the attempts to resolve them will increasingly intersect with Internet governance. Devices with local physical effects are subject to local laws which differ dramatically from place to place. Actors in one locale under one legal regime may act simultaneously across multiple locales where they do not know the local rules. State actors seeking to uphold local rules are likely to bring pressure to bear on the infrastructure of interconnectivity just as they have done with intellectual property.

A too often overlooked policy problem is the long-term environmental impact of the IoT. If the environmental impact of the IoT is mentioned at all, it is usually an optimistic story. For example, a smart thermometer can heat or cool a building according to when it is actually required, reducing the use of energy. Similarly, a smart street light with a sensor can turn on only when needed, reducing the energy it requires. Responsive technologies that meter-out energy, light or water will help reduce human consumption or at least per capita consumption. Automated manufacturing and responsive supply chains promise to reduce waste. But there is also an often forgotten[120] environmental cost to the IoT. As the IoT generates massive amounts of data, that data will mostly be stored in data centers which will in turn demand ever increasing electrical energy to maintain ever increasing data. While many IoT devices are low power, the massive increase in the number of devices that need to be charged or powered will increase demand.[121] Batteries power the new capabilities of many things in the IoT.[122] But if these batteries are not removable, then the usable life of the thing is only the life of the battery. A simple thing such as a water bottle has fewer capabilities than a smart bottle, for example it cannot tell how much water one has drunk because it does not have either circuitry or a battery. But the less capable water bottle might remain useful for decades and even centuries but few batteries are designed to last that long. The life of the battery is then the longest the artifact can be useful, unless the battery can be easily replaced. But the life of IoT devices may not be as long as the batteries last. One result of installing software into things which previously did not

[120] *A too often forgotten problem with the Internet of Things*, STOP AT ZONA-M (Mar. 25, 2018), http://stop.zona-m.net/2018/03/a-too-often-forgotten-problem-with-the-internet-of-things.
[121] Dyani Lewis, *Will the internet of things sacrifice or save the environment?*, THE GUARDIAN (Dec. 11, 2016), http://www.theguardian.com/sustainable-business/2016/dec/12/will-the-internet-of-things-sacrifice-or-save-the-environment; Bonnie Gardiner, *The hidden environmental cost of the Internet of Things*, COMPUTERWORLD (Dec. 8, 2014), https://www.computerworld.com.au/article/561064/hidden-environmental-cost-internet-things; *see also A too often forgotten problem with the Internet of Things*, *supra* note 117.
[122] Mukhopadhyay & Suryadevara, *supra* note 15, at 13.

have software is to tie the life cycle of the thing to software.[123] Repair of the thing will often now require the person engaged in repair to have the skills to re-install or modify software. With the very important exception of some open source software, most software becomes obsolete within a few years. Things which may have been useful for many years will cease to function even if there is nothing physically wrong with them simply because the software is no longer supported. Whether through batteries that will no longer hold charge, or obsolete software, hundreds of types of devices, and millions of devices, will become electronic waste. Electronic waste is much harder to recycle or safely dispose of than most other types of waste due to hazardous and toxic materials.[124] The environmental costs may be reduced by designing, or redesigning devices to enable repair, replacement, and environmentally responsible disposal but how will green design be encouraged? Environmental consequences of the IoT may seem somewhat removed from Internet governance but this account of IoT policy issues would be incomplete without it. Responses to environmental consequences will affect the technologies of the IoT, and thus implicate Internet governance. For instance, an environmentally friendly standard for a type of device may require it to use less power but security concerns may demand that it use more power; the power available to a device affects how it connects with a network, and thus the connectivity protocols it utilizes.

How will Internet governance, reliant as it is on standards and other technical bodies, address the predicaments of privacy, security, and liability raised by the IoT? Standards and the architecture of technology determine how the IoT is configured and how it will be reconfigured in response to these problems. But legal regulation also affects the devices of the IoT. Each device connected to the Internet is subject to multiple overlapping legal regimes which govern how it is controlled and used. For example, a 'smart' toothbrush is subject to the law of property, tort law, consumer protection law, and if it purports to diagnose or treat a medical condition, then it is subject to regulation on the sale of medical devices. Unlike the laws on information, these laws have not been altered to enable the Internet governance regime. These laws apply to the IoT even if the application of any particular rule is unclear and the concurrent application even less clear. There are calls for "permissionless innovation" which would be an extension of the regulatory exceptionalism of the early history of the Internet. The phrase "permissionless innovation" is somewhat hyperbolic since it refers not to a complete absence of restrictions on would be innovators but rather a preference for as few restrictions as possible. But permissionless innovation is not simply a matter of refraining from imposing new regulations on the IoT, instead, it requires law-making, whether through legislatures or courts, that exempts aspects of the IoT from existing laws.

[123] Stacey Higginbotham, *The Internet of Trash: IoT Has a Looming E-Waste Problem*, IEEE SPECTRUM (May 17, 2018), https://spectrum.ieee.org/telecom/internet/the-internet-of-trash-iot-has-a-looming-ewaste-problem.

[124] Mukhopadhyay & Suryadevara, *supra* note 15, at 15.

b) Structuring the Policy Response Space

What is the best way to respond to these problems? Discussions of governance of the IoT often refer to two competing principles around which to structure innovation space, or to organize governance of the IoT policy frontier. One approach, dubbed 'permissionless innovation' is to avoid regulation as much as possible; delaying regulation and relying on technology and consumer-driven market responses to deal with problems, until there is an unarguable case for regulation. Proponents of permissionless information claim it is the successor of the hands-off approach articulated by Werbach.[125] A different approach, "the precautionary principle" requires regulation to preempt harm, especially irrecoverable and diffuse harms.

According to leading proponent, Adam Thierer,[126] permissionless innovation "refers to the general freedom to experiment and learn through ongoing trial-and-error experimentation."[127] Couched in those terms who could be against permissionless innovation?

> If policymakers want to foster the growth of the IoT and get this next technological revolution off to a fast start, they will need to resist the temptation to base policy on worst-case thinking about these technologies. Instead, they should embrace permissionless innovation, just as they did before for the Internet itself.[128]

Thierer maintains that permissionless innovation:

> refers to the tinkering and continuous exploration that takes place at multiple levels—from professional designers to amateur coders; from large content companies to dorm-room bloggers; from nationwide communications and broadband infrastructure providers to small community network-builders. Permissionless innovation is about the creativity of the human mind to run wild in its inherent curiosity and inventiveness. In other words, permissionless innovation is about freedom. [129]

Use of the term "permissionless innovation" is equivocal. Under the current global intellectual property regime, the freedom to engage in permissionless innovation is denied to amateur coders, dorm-room innovators, and small community network builders in key ways. For example, motion sensors, video cameras, audio recorders, and transmission over cellular networks are all well- established technologies. But arranging a motion sensor to trigger a camera and an audio recorder to begin recording, and then having them connect to a cellular transmitter to store the recorded data in a remote server would require permission from the holders of multiple networking, device pairing, and network data storage patents and other rights. Only multinational corporations which have accumulated sufficient patents or other rights so that they can bargain with other multinationals to get licenses have the freedom to innovate, everyone else

[125] ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM 12–15 (2014).

[126] Adam Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J.L. & TECH. 1 (2015).

[127] THIERER, *supra* note 123, at 8.

[128] *Id.* at 18.

[129] *Id.* at 8.

has to get the permission of those with copyright and patents over IoT technologies. Because IoT devices combine a number of different technologies including, radio communication, data processing, sensors, low power computer chips, batteries, no one person or corporation makes all the components of a device, let alone a network. IoT innovation requires interoperability of devices. But interoperability of components and devices routinely requires modification of devices from different manufacturers, sometimes running post- sale software added by a service provider. Modification routinely requires patent and copyright permissions. The most thorough, widespread, and effective constraint on the freedom to tinker and explore is intellectual property. Yet the proponents of permissionless innovation are mostly silent on the barriers to creativity presented by the global intellectual property regime. Some have even defended aspects of the intellectual property regime that are widely regarded as undesirable[130] while others been more equivocal on intellectual property.[131]

Exponents of permissionless innovation do not usually argue for no regulation at all[132] but some powerful actors do seek broad exemption from existing regulatory regimes. Uber, a ride sharing company, sought changes to the usual road rules for its experimental self- driving vehicle program. An executive order issued by the Governor of Arizona in 2015 purported to authorize the operation of a vehicle even if the controller of the vehicle was not in the vehicle.[133] The Governor issued a new order in 2018 after a pedestrian was killed by a driver-less vehicle.[134] The new order made the person testing an unmanned vehicle responsible for compliance with the law. The 2015 order is just one example of "regulatory entrepreneurship." Regulatory entrepreneurship describes the ways in which some new technology corporations attempt, often successfully, to change regulatory environments through exploiting uncertainty about the

[130] Larry Downes, *One Cheer for Patent Trolls*, LARRYDOWNES.COM (Oct. 11, 2010), http://www.larrydownes.com/2010/10/11/one-cheer-for-patent-trolls.

[131] In a 2002 co-edited volume, Thierer, preeminent proponent of permissionless innovation, and copyright scholar Kenneth Crews claim that 'strong' patent and copyright laws are correlated with industrial strength of a country, but concede there is tendency to seek ever more extensive powers through patent and copyright law. Moreover they warn that arguments against intellectual property might undermine arguments for property. Wayne Crews & Adam Thierer, *Introduction* to COPY FIGHTS: THE FUTURE OF INTELLECTUAL PROPERTY IN THE INFORMATION AGE, at xvi–ii (Adams Thierer & Wayne Crews eds., 2002).

[132] For example, Thierer believes that common law privacy protection is likely to prove sufficient for the Internet of Things. Thierer, *supra* note 122, at 40, 70, 101–6; THIERER, *supra* note 123, at 18–19.

[133] Ariz. Exec. Order 2015-09 (2015). The legal effect of this order was not tested, however even if ultra vires it would be make affect the likelihood of action by the organs of the state executive such as the state highway patrol.

[134] Ariz. Exec. Order 2018-04 (2018).

application of existing rules, engage in regulatory arbitrage between geographic and regulatory jurisdictions, and simply become "too big" to regulate.[135]

While the more sophisticated proponents of permissionless innovation do not oppose all regulation, they do oppose the precautionary principle. They agree that new technologies will invariably fail in a variety of ways. However, they propose that since it is impossible in principle to completely predict what these ways will be, which technologies will prove very successful, and which will prove harmful, regulation should only take place once a clear harm has been established. According to proponents of permissionless innovation, even in the face of a clear established harm, regulation should balance interests such as privacy and security against the putative benefits of innovation, efficiency, and consumer choice. The education of consumers, technological fixes, and industry "self-regulation" should be preferred to regulation.[136]

Proponents of the precautionary principle are also concerned with the problem of how to enable innovation while managing risk. Those in favor of the precautionary principle motivate the principle as a way of reducing harms, in particular diffuse and irreversible harms. The precautionary principle was first theorized in the context of environmental regulation.[137] Exactly how the precautionary principle is formulated matters a great deal; it need not be formulated as a rigid requirement for permission but could instead be a requirement that the best available technologies be used to minimize risk.[138] Gilad Rosner and Erin Kenneally who propose a precautionary principle for the IoT, pragmatically concede that "governance and legislation are imperfect mechanisms, and attempts to craft forward-facing consumer protection and privacy rules will be inevitably flawed" but they urge that "[p]rudence is warranted in particular when concerned with democratic harms because they are diffuse and take a long time to manifest and detect."[139]

The precautionary principle could also be invoked to guard against a very different kind of harm, the foreclosure of balanced regulation of a technology. If the deleterious effects of a particular technology are not preempted, then the population subject to those effects may mobilize and require a complete ban of the technology. In addition, a technology could harm a population or demographic but the industry which controls the technology may have acquired such wealth and

[135] Elizbeth Pollman & Jordan M. Barry, *Regulatory Entrepreneurship*, 90 S. CAL. L. REV. 383 (2017).
[136] Thierer, *supra* note 122; THIERER, *supra* note 123.
[137] Richard B. Stewart, *Environmental regulatory decision making under uncertainty*, *in* 20 AN INTRODUCTION TO THE LAW AND ECONOMICS OF ENVIRONMENTAL POLICY: ISSUES IN INSTITUTIONAL DESIGN 71 (2002).
[138] Gilad Rosner & Erin Kenneally, *Clearly Opaque: Privacy Risks of the IoT*, INTERNET OF THINGS PRIVACY FORUM, at 38 (2018), https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf?d8bd54&d8bd54.
[139] *Id.* at 40, 42.

power that it is able to prevent regulation that would prevent or mitigate the harm. If the precautionary principle requires that the best available technologies be used to mitigate risk, this raises the question: what does availability mean? Intellectual property renders the best technologies unavailable except to the rights holder, indeed that is its function. But the rights holder may not be the person best placed to take the precautions required by the precautionary principle. As will be seen in the discussion on patents, which technologies are available, not just to specific actors but available at all is constrained by intellectual property.

Since proponents of permissionless innovation are in favor of some regulation, and those in favor of the precautionary principle wish to preserve space for innovation while curbing harms, it may seem that the two schools of thought are not as far apart as their apparent opposition would indicate. But finding middle ground would not solve the problem of designing the space for innovation. Both schools of thought acknowledge that some failures and unexpected outcomes of technologies are inevitable whether or not there is regulation. A critical question then becomes how policy can shape the space for innovation to "fail well." Cory Doctorow has consistently warned "[h]ow well a system works is only half the picture: the other half is how badly it fails."[140] Failing well includes prompt action to prevent further failure, restoration of the status quo ante where possible, and most importantly, learning from failure to prevent future failure. Technology that prevents users from responding to potential failures is dangerous. Doctorow points out:

> A car is a high-speed, heavy object with the power to kill its users and the people around it. A compromise in the software that allowed an attacker to take over the brakes, accelerator and steering…is a nightmare scenario. The only thing worse would be such an exploit against a car designed to have no user-override…Whatever problems we will have with self-driving cars, they will be worsened by designing them to treat their passengers as adversaries.[141]

We would thus anticipate that regulation of technology would at least, whether it encourages permissionless innovation or employs a precautionary principle, encourage failing well. On close examination, however, we find regulation which criminalizes failing well. One particularly pernicious way in which regulations prohibit failing well is a vague provision of the Computer Fraud and Abuse Act (CFAA) which criminalizes "exceeding authorized access" on a computer.[142] In one case, Patterson Dental, which provided dental practice management software, made private patient data available via a File Transfer Protocol (FTP) server that permitted any client with a password access to all the patient data. Justin Shafer, a security

[140] Cory Doctorow, *Android and iOS both fail, but Android fails better*, THE GUARDIAN (Aug. 9, 2011), https://www.theguardian.com/technology/2011/aug/09/technology-failure-more-important-than-success.
[141] Cory Doctorow, *The problem with self-driving cars: who controls the code?*, THE GUARDIAN (Dec. 23, 2015), https://www.theguardian.com/technology/2015/dec/23/the-problem-with-self-driving-cars-who-controls-the-code.
[142] 18 U.S.C. § 1030 (2012).

researcher, happened on to the server and found the problem and warned Patterson. After the patient data was secure, Shafer and other security researchers announced the breach publicly. Patterson repaid Shafer's kindness by claiming that Shafer had engaged in criminal conduct under the CFAA, and the authorities who apparently did nothing about the failure to safeguard the medical records of 22,000 patients staged a dawn raid on Shafer's house.[143] If anyone who discovers a security flaw is at the mercy of a company with powerful incentives to keep it secret because of vague laws and heedless law enforcement, then neither the companies nor the public will be made aware of the flaws. Ignorance of the flaws will not prevent bad actors from using the flaws for their own personal gain, but it will prevent people from taking remedial action. The CFAA is not the only law which criminalizes security research; §1201 of the Digital Millennium Copyright Act[144] can be used to prosecute anyone who demonstrates a flaw in a software security system if that system can be construed as a protection measure intended to prevent copying of that software. These laws, and others like them in jurisdictions around the world, distort the space for failing well and thus innovation. They both prevent permissionless innovation and discourage precaution. That is not all, as Doctorow points out, "the main event is not user rights or innovation: it is security and free speech."[145] Anti-circumvention law, such as DMCA §1201, is a central feature of the global intellectual property regime. What does this regime portend for the IoT?

II. The Global Intellectual Property Regime Meets IoT

A. The Global Intellectual Property Regime

Just as Internet governance can be described as a regime, so too can global intellectual property. The Internet governance regime, characterized far less by treaties and other laws and more by private actors, standards bodies, and nation states through indirect roles, contrasts starkly with the global intellectual property regime that is dominated by treaties, international intergovernmental organizations, and nation states actors. The global intellectual property regime seems ill configured to respond to the challenges presented by the IoT, both to intellectual property rules and to the many instances in which intellectual property rules constrain policy responses to critical challenges, such as privacy, security, and liability. The history of uneasy interaction between global Internet governance and the global intellectual property regime seems similarly unpromising for addressing IoT challenges. The IoT threatens to bring the unresolved tension between Internet governance and the global intellectual property regime to a head. This analysis is accompanied by the oft-repeated caveat that the phrase

[143] Dissent Doe, *FBI raids dental software researcher who discovered private patient data on public server*, DAILY DOT (May 27, 2016), https://www.dailydot.com/layer8/justin-shafer-fbi-raid.
[144] 17 U.S.C. § 1201 (2012).
[145] Cory Doctorow, *I Can't Let You Do That, Dave*, 58 COMMUN. ACM 41 (2015).

"intellectual property" may lead to confusion, both by suggesting a stronger link to property in physical things than is borne out on closer analysis and by relegating the different legal schemes of copyright, patent, trademark, trade secrets, and designs into a single crude receptacle.[146] I use the term "intellectual property" here neither to assert a claim that the different legal schemes share some essential nature nor to gloss over the differences between the different systems schemes, but simply because the international rule making and enforcement system, which I analyze here, is identified with reference to the phrase intellectual property and cannot be easily described without using the term.

Ostensibly, the primary venue for intellectual property rule making is the World Intellectual Property Organization (WIPO), a United Nations body headquartered in Geneva. But WIPO is not the only, or even the most powerful, venue for the creation of international intellectual property rules. Instead, intellectual property has been characterized by the movement first from multi-lateral treaty negotiations at WIPO and through the World Trade Organization (WTO), then to bi-lateral trade agreements, often referred to as Free Trade Agreements (FTAs), and then to so called 'plurilateral'[147] agreements, such as the failed Anti-Counterfeiting Trade Agreement (ACTA) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), formerly known as the Transpacific Trade Partnership (TPP). Bi-lateral trade agreements have tended not to introduce new categories of rules, but instead have tended to increase term lengths and require more stringent enforcement measures. The literature on the global intellectual property regime refers to these movement from multi-lateral agreements to bi-lateral and so on as "forum shifting" and traces how it is initiated by the *demandeur* states seeking ever more exacting intellectual property rules.[148] Intellectual property is also characterized by strategic "regime shifting" from international agreements to national regulation and back.[149] Together these movements result in a 'global IP upward ratchet' of ever increasing powers for those awarded rights by the regime, and ever increasing demands on states to use their resources to enforce private rights.[150] But it would be artless to understand the global intellectual property regime as essentially the maneuvering of nation states for competitive

[146] For a discussion of the confusion around the term and the appropriateness of using it see JAMES BOYLE, THE PUBLIC DOMAIN: ENCLOSING THE COMMONS OF THE MIND 7–8 (2008).
[147] For a discussion of the term 'plurilateral' see Andrew Rens, *Enforcement Theater: The Enforcement Agenda and the Institutionalization of Enforcement Theater in the Anti-Counterfeiting Trade Agreement*, 35 SUFFOLK TRANSNAT'L L. REV. 553, 559 (2012).
[148] Susan K. Sell, *TRIPS Was Never Enough: Vertical Forum Shifting, FTAS, ACTA, and TTP*, 18 J. INTELL. PROP. L. 447 (2011).
[149] Laurence R. Helfer, *Regime Shifting: The TRIPs Agreement and New Dynamics of International Intellectual Property Lawmaking*, 29 YALE J. INT'L L. 1 (2004); Laurence R. Helfer, *Regime Shifting in the International Intellectual Property System*, 7 PERSP. ON POL. 39 (2009).
[150] Susan K. Sell, *The Global IP Upward Ratchet, Anti-Counterfeiting and Piracy Enforcement Efforts: The State of Play*, AM. U. WASH. C.L. DIGITAL COMMONS PIJIP RES. PAPER SERIES 1 (2010).

advantage. Peter Drahos and John Braithwaite describe how the negotiation of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), a central feature of the regime, was at the behest of knowledge cartels which operate globally.[151]

The strongest rules in the international intellectual property regime are in TRIPS.[152] Since TRIPS was part of the Uruguay round of the Global Agreement on Trade and Tariffs, it is under the auspices of the World Trade Organization rather than WIPO. Since disputes about TRIPS can be referred to the World Trade Organization dispute process, in which a successful state can impose trade penalties on a state found to have failed to comply with its obligations, TRIPS has considerably greater force than WIPO treaties. The species of intellectual property in TRIPS include copyright, patent, trademark, trade secrets, and designs. There are other legal schemes that are not featured in TRIPS but are often referred to as intellectual property, including database rights, traditional knowledge (TK), and Geographical Indications. Only one of these has immediate import for the IoT—'database rights', where the legal scheme is largely confined to the European Union. TRIPS requires participating countries to comply with the Berne Convention for the Protection of Literary and Artistic Works (except for the requirements to protect the moral rights of authors) and the Paris Convention for the Protection of Industrial Property. But TRIPS also sets out requirements of its own. Because countries which are accused of non-compliance with TRIPS can be subject to dispute resolution and possibly trade sanctions under the auspices of TRIPS, the years since TRIPS came into force on January 1, 1995 have seen powerful pressure on countries to change their intellectual property laws to prevent claims of non-compliance.[153] In addition to TRIPS and the treaties it subsumes, the World Intellectual Property Organization Copyright Treaty (WCT),[154] which came into force in 2002, substantially determines policy for the IoT even though the IoT was not yet envisaged at the time it was negotiated in the mid– 1990's. The WCT altered the global intellectual property regime in a number of significant ways. It required countries to extend copyright to software (Article 4), and to grant an exclusive right over compilations of data "which by reason of the selection or arrangement of their contents constitute intellectual creations" (Article 5). Authors of literary and artistic works (and thus their successors in title) are to be granted exclusive control over the distribution of copies of their works (Article 6) and of making their works

[151] PETER DRAHOS & JOHN BRAITHWAITE, INFORMATION FEUDALISM: WHO OWNS THE KNOWLEDGE ECONOMY?, 48-60, 128, 150–80 (2002).

[152] TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) [hereinafter TRIPS Agreement].

[153] TRIPS and its re-founding of the global intellectual property regime is the subject of an extensive literature. Leading texts include DRAHOS & BRAITHWAITE, *supra* note 148, and CAROLYN DEERE, THE IMPLEMENTATION GAME: THE TRIPS AGREEMENT AND THE GLOBAL POLITICS OF INTELLECTUAL PROPERTY REFORM IN DEVELOPING COUNTRIES (2009).

[154] WIPO Copyright Treaty, *adopted* Dec. 20, 1996, WIPO Doc. CRNRIDC/94 [hereinafter Copyright Treaty]; WIPO Performances and Phonograms Treaty, *adopted* Dec. 20, 1996, CRNR/DC/95.

available to the public (Article 8), and authors of computer programs are to be granted the right to license their works. Signatory countries are obliged to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures…used by authors…that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law" (Article 11). Technological measures primarily refer to software that prevents copying or changing software or other digitally encoded information. Signatories are also required to "provide adequate and effective legal remedies against any person knowingly" removing or altering electronic rights management information, which is information that identifies the author, owner, or terms of use (Article 12). Knowingly distributing copies with altered electronic rights management information must similarly be subject to legal remedy. The WCT does not require that circumvention of technological measures, sometimes also referred to as technical protection measures (TPMs) measures and changes to electronic rights management information be criminalized, but it has been used as the justification by countries that have criminalized these activities.[155]

Both TRIPS and the WCT permit exceptions and limitations to their provisions but only "in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author."[156] This constraint has been subject to conflicting interpretations,[157] but even its most generous interpretation is a far cry from the flexibility of Internet governance norms. This difference is typical of the divergence between the regimes. The intellectual property regime relies on treaties, and organizations that administer treaties, and is instantiated through national laws, primarily statutes. Although there are exceptions and limitations intended to add flexibility these are both constrained and contested. Rather differently, the global Internet governance regimes relies on non-governmental bodies, such as standards bodies, and relies for its implementation on technical protocols. The setup of the regimes thus repeats the preference for avoiding regulation for the Internet in the US, except when it comes to intellectual property, leading developing world participants in global Internet governance to ask why governments in the global North have sought a global Internet governance regime that eschews strong legal demands on states and a global intellectual property regime characterized by strong legal demands on states.[158] Despite the differences, Internet

[155] Title I of the Digital Millennium Copyright Act is titled "WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998." WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998, S. 2037, 105th Cong., tit. I § 103. §1204 of that title criminalizes circumvention while §1203 grants statutory damages. 17 U.S.C. §§ 1203, 1204 (2012).
[156] WIPO Copyright Treaty, art. 10, *supra* note 151.
[157] Max Plancke Declaration on a Balanced Interpretation of the 'Three Step Test' in Copyright Law. and Christophe Geiger et al., *Declaration on a Balanced Interpretation of the "Three-Step Test" in Copyright Law*, 39 IIC 707 (2008).
[158] Cogburn, *supra* note 53, at 41.

governance, like the global intellectual property regime, has been a locus of successful efforts to increase the power of intellectual property right holders.

Internet infrastructure control points have also increasingly become adapted for enforcing intellectual property rights online. Technological advancements such as the ease and minimal cost of distributing, replicating, and storing digital media online, as well as the rise of distributed peer-to-peer file sharing systems, have upended the traditional business models of media content industries and significantly complicated modes of intellectual property rights enforcement. "Content industries have traditionally enforced copyright protection by either prosecuting individuals suspected of illegally sharing copyrighted material online or via approaches that request the takedown of specific infringing content . . . ."[159]

Ways in which assertions of intellectual property rights have been enforced through Internet infrastructure include domain name blocking and algorithmic filtering.[160] Algorithmic filtering and take down shows what is at stake. Many technology corporations that allow users to upload digital files such as videos use automated blocking and take down systems apparently to avoid enabling copyright infringement. These increasingly rely on algorithms to identify whether a digital file is a copy of another which is claimed to be subject to copyright. As Maayan Perel and Niva Elkin Koren observe:

> Algorithmic enforcement by online intermediaries reflects a fundamental shift in our traditional system of governance. It effectively converges law enforcement and adjudication powers in the hands of a small number of mega platforms, which are profit-maximizing, and possibly biased, private entities. Yet notwithstanding their critical role in shaping access to online content and facilitating public discourse, intermediaries are hardly held accountable for algorithmic enforcement. . . . [A] lgorithmic copyright enforcement by online intermediaries lacks sufficient measures to assure accountability, namely, the extent to which decision makers are expected to justify their choices, are answerable for their actions, and are held responsible for their failures and wrongdoings.[161]

The result is automated systems that effectively decide issues of ownership, authorization, and legality in opaque processes that lack "transparency, due process and public oversight."[162]

Aram Sinnreich points out that even if algorithms take into account whether a use was de minimis or fair use, making such judgments the function of software rather than humans threatens to replace not simply the law but humans as makers of culture.[163] He warns that the

[159] DeNardis & Musiani, *supra* note 32, at 14.
[160] For an analysis of specific examples see DeNardis, *supra* note 45.
[161] Maayan Perel & Niva Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, 19 STAN. TECH. L. REV. 473, 473–74 (2016).
[162] *Id.* at 532.
[163] Aram Sinnreich, *Four Crises in Algorithmic Governance*, ANN. REV. OF LAW & ETHICS 181, 183 (2018).

inscrutability of the algorithmic processes employed by profit seeking corporations conceals the collapsing of the separation of powers; they set the standard of what constitutes infringement, judge specific instances and enforce those judgments.[164] While communications intermediaries have tended to adopt algorithmic filtering in response to pressure from corporations with large numbers of video or music copyrights, it is may soon be required by law in some jurisdictions. The Digital Single Market Directive, approved by the European Union in early 2019, includes controversial provisions in Article 13 which mandate automated filtering. Although the current formulation does not explicitly require automated filtering, copyright experts, including Pamela Samuelson, anticipate that there will be industry pressure to interpret the provision as effectively requiring automated filtering.[165]

Is the replacement of legal processes by technological processes the extension of the global intellectual property regime through other means? Or is it replacement of the global intellectual property regime itself? Either way it seems likely there will be increasing efforts to co-opt the technical infrastructure of the IoT to increase the power of intellectual property rights holders. Unlike technological processes the texts of international intellectual property treaties are not self-executing. Instead each country passes national laws which must at a minimum include the rules in the treaties but can go beyond them. Those laws are then interpreted and applied by courts which can result in laws which are extreme forms of a treaty. In the United States patent, copyright and trade secrets law has tended to develop in ways that limit the space for policies governing the IoT. These tendencies are neither necessary nor inevitable consequences of the treaties, so they may be reversed or at least checked. Jurisdictions that have intellectual property laws which tend to foreclose on policy options for the IoT can change those laws to open up policy options without automatically encountering problems with the treaties. But even if those jurisdictions do not change then at least jurisdictions where these tendencies are not as pronounced may make use of the existing flexibilities in the treaties to establish policy space for governance of the IoT.

B. Patent Problems

The global intellectual property regime requires that patents be granted, with a few exceptions, for new technologies.[166] A wide variety of patents affect the IoT, including patents on network resource management, communications protocols, routing algorithms, image processing, and sensors.[167] Not all of these patents relate solely or primarily to the IoT. But some patents do

[164] *See id.* at 185–89.
[165] Pamela Samuelson, *The EU's Controversial Digital Single Market Directive*, 61 COMMUN. ACM 20, 22 (2018).
[166] The most significant provision in this respect is Article 27 of TRIPS. *See* TRIPS AGREEMENT, *supra* note 149, Art. 27.
[167] See LEXINNOVA, *Internet of Things: Patent Landscape Analysis* 4–5.

address IoT specific issues for example, a "method of profiling a physical environment via Internet of Things (IoT) devices connected via an IoT integration platform"[168] or in other words, a system for enabling IoT devices to identify and keep track of objects, such as people, in their environments. As this example shows, patents for the IoT are likely to be sought not for an individual component, which may already be subject to multiple patents, nor even for the interaction of components in a thing, but for the interactions of several things with each other such as a network and their environment. As a result, IoT patents are likely to be increasingly abstract and constituted by the behavior of software. This has caused at least one commentator to warn that the IoT will affect the patent system:

> [T]he Internet of Things (IoT) will lead to a dramatic increase of applications for software patents and if examiners, courts and legislators are not careful, there is a concrete risk of a surreptitious generalised grant of patents for computer programs as such (in Europe) and for abstract ideas (in the US).[169]

Perhaps technology will change in the future so that making an IoT device will no longer require multiple components and technical specifications to be provided by different manufacturers. But, at the time of writing, most reasonably sophisticated IoT devices must include components from a number of different manufacturers and must comply with the technical specifications of those components to make them interoperate. Once an IoT device is connected to a network, this complexity tends to repeat, and it must frequently interoperate with an assortment of devices. A manufacturer or network operator must figure out how to get all of these to work together effectively. If, at the same time, many of these components and technical specifications are subject to patents, then there is a double workload; a project must not only get the technology to work together, but it must obtain permission from all of the patent holders whose patents may apply to the technology. That includes not only patents that describe how a specific component, such as an antenna, is constructed but also patents over methods of routing information between devices and over software, in jurisdictions that permit those patents, such as the United States. When two manufacturers both hold patents that the other desires to license they can enter into a cross-licensing agreement. However, a patent holder may not need any licenses because it does not produce goods or services. Patent holders that do not themselves produce any technology but simply collect royalties are sometimes referred to as non-practicing entities (NPE's) or patent assertion entities (PAE's)[170] or sometimes more plainly, patent trolls.[171] A patent holder may

[168] U.S. Patent No. 9,871,865 B2, at [57] (filed Jun. 25, 2014).
[169] Guido Noto La Diega, *Software Patents and the Internet of Things in Europe, the United States and India*, 39 EUROPEAN INTELL. PROP. REV. 173, 173 (2017).
[170] Daryl Lim, *Patent Holdups*, *in* THE CAMBRIDGE HANDBOOK OF ANTITRUST, INTELLECTUAL PROPERTY, AND HIGH TECH 245, 247 (Roger D. Blair & D. Daniel Sokol eds., 2017).
[171] Although the term is sometimes contested, it is used in some scholarly literature, for example Ahmed J. Davis & Karolina Jesien, *The Balance of Power in Patent Law: Moving towards Effectiveness in Addressing Patent Troll Concerns*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 835 (2012).

seek to extract revenue rather than engage in cross licenses from its patents. The manufacturer or other technology provider intent on creating a new technology will likely have pay for a license. But a patent holder may simply refuse a license, or the holder may offer it on terms which make it financially infeasible for a technology provider to obtain. Even if a license fee seems reasonable, a number of license fees together can make producing a product too expensive to create; this is called royalty stacking. A patent holder can get a court order to prevent the distribution of a product even after a manufacturer has invested heavily in a product. This practice, called "patent holdup," "can enable a patent holder to negotiate royalties far in excess of the patent holder's true economic contribution."[172] Either patent holdup or royalty stacking may prevent a product or service from being introduced.

While patent hold up may prevent some products or services from becoming available, patents can sometimes have even more severe effects on innovation. When multiple players each hold patents over an essential piece of the technology so that each can prevent the others from creating the whole technology, then each player has an incentive to hold out for a greater share of the royalties. As a result, no player can create the technology because each player can prevent the others. This is known as patent gridlock.[173]

Research on the IoT patent landscape shows it includes many highly capitalized corporations but also multiple patent holders.[174] Widespread patent activity likely indicates substantial investment into new technologies for the Internet of Things. However, there is also a high risk of IoT patent litigation, especially with respect to wireless protocols.[175] Why should the IoT be particularly susceptible to these dangers? Essential to the functioning of the IoT is the interconnection of devices. Interconnection is accomplished through technical standards.[176] A single device might include multiple components, each of which must conform to one or more standards. In turn, each standard might implicate a number of patents. To enable the creation of a technical standard, the participants in a standards body will negotiate terms for anyone implementing the standard. These standard terms include patent licenses but only to implement the standard. Implementation terms often specify access will be on a Fair, Reasonable, And Non-Discriminatory (FRAND) basis. This may require a royalty that should be fair, reasonable and non-discriminatory, but the way that the royalties are to be determined is often not specified in the standard nor by the standards organization. Some experts regard FRAND as intrinsically

[172] Mark A. Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking*, 85 TEX. L. REV. 1991, 1993 (2007).
[173] *See* MICHAEL HELLER, THE GRIDLOCK ECONOMY: HOW TOO MUCH OWNERSHIP WRECKS MARKETS, STOPS INNOVATION, AND COSTS LIVES 49–78 (2008).
[174] *See* LEXINNOVA, *supra* note 164, at 1, 4–5.
[175] *Id.* at 1, 13 (noting the intensity of litigation for wireless protocols).
[176] Jason R. Bartlett & Jorge Contreras, *Rationalizing FRAND Royalties: Can Interpleader Save the Internet of Things?*, 36 REV. LITIG. 285, 286–87 (2017).

underdetermined.[177] As a result, royalty stacking and patent holdup may haunt the implementation of a technical standard even if patent royalties are in principle fair, reasonable, and non-discriminatory.[178] Widely adopted wireless interconnection standards implicate thousands of patents.[179] These issues make IoT development particularly vulnerable to the risks of royalty stacking and patent hold up.[180]

One way to resolve disputes over the royalties to be paid for patent permission needed to comply with a standard is through litigation. Licenses for one party to use a technology patented by another tend to specify precise amounts or percentages for royalties. But FRAND terms on standards do not often offer such specificity and seem structurally predisposed to litigation. However, litigation tends to exacerbate, rather than resolve, the underlying structural issues.[181] Jason Bartlett and Jorge Contreras have shown that courts in the United States have failed to develop an appropriate methodology for valuing all the patents in a standards related patent dispute, and instead courts tend to overvalue the patents in dispute.[182] Competing court decisions using a flawed valuation methodology could award royalties greater than the gross profit from a product. Bartlett and Contreras suggest an ingenious, though convoluted, solution. A producer of a product can use federal interpleader rules. Interpleader is an option in US federal procedural law that enables a participant in legal proceedings to require others to join those legal proceedings. US. interpleader is a flexible rule, which may be used to avoid multiple lawsuits regarding the same issues. A producer can use interpleader to summon all the affected patent holders to court for a determination of their aggregate royalties.[183] Since all potential royalty claims are before a court, that court will be better placed to avoid the "inconsistent and

[177] Eli Greenbaum notes that "[t]he FRAND commitment is, almost by definition, incomplete." Eli Greenbaum, *Forgetting FRAND: The WIPO Model Submission Agreements*, LES NOUVELLES 81, 86 (2015).

[178] *See* Bartlett & Contreras, *supra* note 173, at 290–91.

[179] *See id.* at 288–89.

[180] Fiona Scott Morton and Carl Shapiro warn that "the 'Internet of Things' is a new and growing area where royalty stacking and patent holdup appear to be very real dangers. Devices of all sorts, from thermostats to railroad cars to refrigerators, are being given connectivity using standards developed by SSOs. The price of those chips, and whether the IP contained in them costs $5 or $0.50 or $0.005, will determine the nature of new applications and the rate of adoption. Failure to prevent patent holdup relating to tomorrow's information technology and communications standards is likely to cause significant social welfare loss in the years ahead." Fiona Scott Morton & Carl Shapiro, *Patent Assertions: Are We Any Closer to Aligning Reward to Contribution?*, *in* 16 INNOVATION POLICY AND THE ECONOMY 89, 124 (William R. Kerr et al. eds., University of Chicago Press 2016).

[181] *See* Bartlett & Contreras, *supra* note 173, at 297–98.

[182] *Id.* at 293–305.

[183] *Id.* at 306–32.

incongruous results" of ad hoc claims.[184] Ingenious as this is, it does not represent a global solution. The proposed solution would operate only within one jurisdiction. United States federal interpleader rules are unique. Other legal systems have their own rules on joining parties to litigation that do not equate easily with U.S. federal interpleader rules, which means that the solution cannot be easily replicated. Because supply chains are global, some technology providers may have no presence in the United States and so cannot be brought to court, but they may exercise their rights in other jurisdictions. The deployment of interpleader for a single calculation of royalties requires a potential target of patent royalty claims to proactively engage in costly legal proceedings in the hope that its royalty burden will be reduced.

If interpleader is too idiosyncratic to present a solution for an entire standard, what is the alternative? Competition regulation prohibits large-scale coordination between industry actors. However, coordination around technical standards enables innovative products and is given a free pass. Authorities can refuse a free pass to standards where royalty stacking and patent holdup are likely to occur. From an antitrust point of view, open standards, which are by definition royalty-free rather than FRAND, should be regarded as benign. So too should standards that require participation in defensive patent schemes, such as the Open Invention Network (OIN).[185] OIN represents a new kind of large-scale collaboration that is becoming increasingly important. For example, Microsoft, a longtime opponent of open source, recently joined OIN[186] in which participants agree not to assert patents that bear on the Linux core against participants who have made a similar pledge.

But FRAND patent terms for participation in a standard should attract regulatory attention. FRAND is especially problematic if the standards organization and its participants cannot point to measures that will prevent royalty stacking and patent holdup. One measure that could avoid royalty stacking is a binding independent mechanism for calculating the total royalties of a product. Another measure could be a binding undertaking not to apply for injunctive relief, which is a powerful threat used for patent holdup. Instead, however, participants should commit to simply claim royalties. Competition enforcement is ex-post, but it could have an ex-ante effect. Once industry players become aware of the kinds of standards agreements that attract regulatory scrutiny, they will have reason to prefer standards arrangements that do not. By paying attention to royalty stacking and patent holdup as anti-competitive behavior, regulators can, without either setting standards or coordinating across borders, nevertheless, encourage global standards that avoid these ills.

[184] *Id.* at 333.

[185] OPEN INVENTION NETWORK, https://www.openinventionnetwork.com (last visited Dec. 13, 2018).

[186] *Microsoft Joins the Open Invention Network Community*, OPEN INVENTION NETWORK (Oct. 10, 2018, 10:00 AM), https://www.globenewswire.com/news-release/2018/10/10/1619375/0/en/Microsoft-Joins-the-Open-Invention-Network-Community.html.

Does the global intellectual property regime contain possibilities for addressing royalty stacking and patent holdup in the IoT? WIPO runs the Arbitration and Mediation Center, which offers alternative dispute resolution services for international and cross-border disputes that require intellectual property expertise. In 2013, the Center published model agreements for the submission of FRAND disputes to the Center. However, on closer examination, the institutional constraints on the Center have rendered arbitration under the model agreements no better suited to resolving FRAND disputes than national courts. The model agreements may be required as part of the negotiation of patent terms for a standard or required at the time of a dispute. Arbitration requires the agreement of each party in a dispute for it to be arbitrated. Therefore, a party that believes that arbitration is likely to find against it can refuse arbitration, or require that the arbitration agreement gives some kind of advantage in arbitration proceedings.[187] This feature of arbitration also makes it far less likely that all the members of a standards organization with patents that bear on a standard would participate in the dispute. The agreements do not specify that the process must set specific royalty and license terms, just a range of reasonable rates and terms.[188] Because the agreements do not specify whether the arbitrators calculate royalties (or royalty ranges) for disputed patents in isolation or taking into account all the patents bearing on standard,[189] they do not provide a solution for royalty stacking. Since the agreements also make any awards confidential by default,[190] they also prevent the awards from informing other royalty negotiations by other parties to the standards, which would in turn reduce the costs and uncertainty of more disputes. Although the agreements do not prevent parties in arbitration from seeking injunctions in national courts, they do prevent them from raising the invalidity of the disputed patents in national courts. As a result of the WIPO Arbitration and Mediation Center model, FRAND submission agreements do not offer a solution to the systematic problems of royalty stacking and patent hold up that hinder IoT innovation. There is some, albeit faint, hope that the issue may be addressed by the WTO.[191] In Article 8.2 TRIPs permits members to take measures "to prevent the abuse of intellectual property rights… or the resort to practices which unreasonably restrain trade or adversely affect the international transfer of technology." Article 31 of TRIPS allows for the issue of a compulsory license when "the proposed user has made efforts to obtain authorization from the right holder on reasonable commercial terms and conditions and that such efforts have not been successful within a reasonable period of time."

[187] Greenbaum, *supra* note 174, at 83, 87.

[188] *Id.* at 86.

[189] *Id.*

[190] *Id.* at 83.

[191] In a WTO working paper, Xiaoping Wu identifies open standards, patents pools, and courts refusing injunctive relief as possible means of addressing royalty stacking and patent hold up, but does not endorse them as policy solutions. Xiaoping Wu, *Interplay between Patents and Standards in the Information and Communication Technology (ICT) Sector and its Relevance to the Implementation of the WTO Agreements* (WTO Working Paper ERSD-2017-08, 2017).

Article 40.2 of TRIPS permits members to identify "licensing practices or conditions that may in particular cases constitute an abuse of intellectual property rights having an adverse effect on competition in the relevant market." While these articles give member countries the possibility of addressing the problems of patent- encumbered standards, a country that implements a novel regulatory solution risks a costly dispute process at the WTO. This risk would be mitigated by a treaty or model law which designates certain measure as indisputably permitted under TRIPS. Yet while the global intellectual property regime holds these formal possibilities for addressing the patent problems threatening the IoT, years of discussion about patents and standards at the WTO since 2005 have not led to any progress on the issues.[192]

If the global intellectual property regime seems unlikely to respond to the IoT's patent problems, then how could Internet governance address them? Standards organizations play such a prominent role in Internet governance since technologies depend on standards to work together. Standards bodies may be able to set standards terms to resolve these problems. Many standards important to the Internet are royalty free,[193] but hardware manufacturers are often more familiar with FRAND. Standards organizations are thus potential sites to address these issues, but without external pressure to cooperate, industry participants face a collective action problem.

C. Copyright and Anti-Circumvention

The global intellectual property regime is most substantive when it deals with copyright. Through the WCT, the regime now includes prohibitions on circumventing digital locks. Discussing the combined effect of TRIPS and the WCT for international copyright Jane Ginsburg concludes:

> "International copyright" can no longer accurately be described as a "bundle" consisting of many separate sticks, each representing a distinct national law, tied together by a thin ribbon of Berne Convention supranational norms. Today's international copyright more closely resembles a giant squid, whose many national law tentacles emanate from but depend on a large common body of international norms.[194]

Three intertwined developments have come to vastly extend the power that copyright law gives a copyright holder over the owners of physical things which incorporate their software 1) the

[192] Wu refers to discussions on the issues of royalty stacking and patent holdup dating back to least 2008 in both the committee on the Agreement on Technical Barriers to Trade (TBT committee) and the TRIPs Council, but in the last ten years no apparent progress has been made. *See id.* at 24–26. This contrasts unfavorably with the speed at which the Uruguay round of negotiations resulted in the entire TRIPS agreement as an annex to the Global Agreement on Trade and Tariffs (GATT).

[193] For example, the World Wide Web consortium requires that contributions to standards be licensed royalty free, *Patent Policy*, W3C (Aug. 1, 2017), https://www.w3.org/Consortium/Patent-Policy-20170801.

[194] Jane C. Ginsburg, *International Copyright: From a Bundle of National Copyright Laws to a Supranational Code*, 47 J. COPYRIGHT SOC'Y U.S.A. 265, 289 (2000).

licensing of software instead of sale of goods such as books, 2) license agreements which double as contracts which purport to restrict how owners can dispose of their own property, and 3) anti-circumvention rules that prohibit, and even criminalize, owners from modifying and repairing their own property.

Providers of 'proprietary software'[195] increasingly claim that they do not sell a copy of the software to a purchaser but rather that they license the use. As a result, a purchaser is not entitled to continue using the software the way a person who buys a book is entitled to keep reading it after buying it; instead, the licensee can only use the software for as long as the license permits. While someone who has bought a book can sell it or give it to someone else, a licensee typically cannot pass the license on to another. Together these have undermined exhaustion, which in the United States is known as the first sale doctrine. Now that software is incorporated into a growing number of objects which would become unusable without it, this restriction on ownership that was confined to software is being spread to a wide range of things. For example, a child's teddy bear could be handed down from one generation to the next, given to an underprivileged child, or used in an art project. But once a computer chip and WiFi connectivity are added, each of those acts may give rise to legal problems. The company that owns the software may cease to support it after a few years. It may still function, but without updates become increasingly insecure and a potential hazard. The software license may not be transferable to another person so that someone given the teddy bear may find themselves inadvertently, even unknowingly infringing copyright.[196] Modifying the sounds the teddy bear makes, or preventing it from recording the child who plays with it, may infringe copyright or even constitute criminal circumvention of a technical protection measure. The balance between rights of ownership in physical artifacts and copyright over knowledge embedded in those artifacts has been replaced, eviscerating ownership.[197]

Linked to this is a trend in the United States of software licenses containing contractual restrictions on usage and transfer of property.[198] This combination of license and contract is known by the unlovely title of an end user license agreement (hereafter 'EULA'). An EULA is

[195] That is software which is not available under a Free or Open Source (FOSS) license.
[196] Deidre Mulligan cites several examples of software licensing terms that purport to restrict the use or resale of devices, including the license for Google Glass which forbade resale or indeed giving the product to anyone else. Christina Mulligan, *Personal Property Servitudes on the Internet of Things*, 50 GA. L. REV. 1121, 1122–24 (2016); s*ee also* Stacey-Ann Elvy, *'Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software'* WASH. & LEE L. REV. 77 (2017).
[197] Aaron Perzanowski & Jason Schultz, *Reconciling Intellectual Property and Personal Property*, NOTRE DAME L. REV. 1211 (2015); *see* PERZANOWSKI ET AL., *supra* note 115.
[198] Molly Van Houweling, *The New Servitudes*, GEOR. L.J. 885 (2007); Christina Mulligan, *Licenses and the Property/Contract Interface*, SSRN Scholarly Paper ID 2987325 (Social Science Research Network), Sept. 18, 2017.

not the ideal agreement of common law contract doctrine: a mutual understanding reached by two parties with equal bargaining power. Instead an EULA is imposed, without possibility for negotiation, by a provider of technology, and is unlikely to be read or comprehended by the purchasing party. While the entitlements of an owner in respect of her property are well established not just in law but also in public consciousness, each EULA contains complicated, usually variable provisions. Owners of EULA encumbered devices are left uncertain about what they may do or not do with their property. Uncertainty increases transaction costs and thus increases economic inefficiency.[199] When the legislature grants exclusive control over certain acts to copyright holders it strikes a balance between the rights of those holders and those who use products subject to copyright. Copyright holders can grant licenses others to perform the exclusive acts. But when copyright holders include in those licenses additional limitations on use of the product, limitations that are not found in copyright law, then they are attempting to upset the balance set by the legislature. Courts could maintain the balance set by the legislature by refusing to enforce those terms. But often they fail to do so.[200] In the United States, there is no settled consensus on the extent to which EULAs are enforceable.[201] A growing trend is for EULAs to forbid owners from modifying or repairing their own property. Owners may also be restricted in their ability to modify or repair their property by technical barriers installed by manufacturers. But if an owner is willing to risk being sued under a EULA and has the skill to overcome the technical barriers, she faces a third hazard; anti-circumvention law, which routinely criminalizes the act of overcoming the technical barrier and thus in effect criminalizes an owner modifying her own things.

What became anti-circumvention provisions were first discussed at WIPO in 1989,[202] prior to the creation of the World Wide Web and before widespread global connectivity. When the WCT was being negotiated, intermediaries reliant on copyright justified the need for new incursions into the power of owners of their property by pointing to what they claimed[203] was widespread copying of the physical discs on which music and software were stored in digital form.[204] The

[199] The MIT Press, The End of Ownership 7–9.

[200] David Nimmer et al., *The Metamorphosis of Contract into Expand*, 87 CAL. L. REV. 17, 29–34, 76–7 (1999).

[201] For a recent summary of the cases and scholarship see Guy A. Rub, *Copyright Survives: Rethinking the Copyright-Contract Conflict*, 103 VA. L. REV. 1141 (2017).

[202] Ian Brown, *The Evolution of Anti-Circumvention Law*, 20 INT'L REV.L., COMPUTERS & TECH. 239, 241 (2006).

[203] Despite the sustained amplification of these claims there is little in way of evidence for them. *See* Giancarlo F. Frosio, *Digital Piracy Debunked: A Short Note on Digital Threats and Intermediary Liability*, INTERNET POLICY REVIEW (2016).

[204] For a typical example of this narrative, see Jeffrey P. Cunard et al., *Current Development in the Field of Digital Rights Management*, Background 9–13 (Standing Committee on Copyright and Related Rights, World Intellectual Property Organization), May 4, 2004. S*ee also* Brown, *supra* note 199, at 242–43.

proposed solution was to prevent copying by encrypting the digital copy and allowing decryption only for certain uses. But as Cory Doctorow points out, this resulted in a fatal design flaw in technical protection measures:

> In DRM, the attacker is *also the recipient*. It's not Alice and Bob and Carol, it's just Alice and Bob. Alice sells Bob a DVD. She sells Bob a DVD player. The DVD has a movie on it – say, Pirates of the Caribbean -- and it's enciphered with an algorithm called CSS -- Content Scrambling System. The DVD player has a CSS un-scrambler...But there's the rub. Alice wants Bob to buy Pirates of the Caribbean from her. Bob will only buy Pirates of the Caribbean if he can descramble the CSS-encrypted VOB -- video object -- on his DVD player. Otherwise, the disc is only useful to Bob as a drinks-coaster. So Alice has to provide Bob -- the attacker --with the key, the cipher and the ciphertext...At the end of the day, all DRM systems share a common vulnerability: they provide their attackers with ciphertext, the cipher and the key.[205]

Since the technological solution was inherently unworkable, the music and movie industries demanded a law which prohibited the breaking of the locks.[206] But the law also applied to software. Though the manufacture and sale of compact discs appear to be in terminal decline,[207] in the IoT, software is being incorporated into many more types of physical objects. Thus, anti-circumvention law then applies to those objects.

The sweeping prohibitions on circumvention in the DMCA do have a few narrow exemptions, such as permission to circumvent technical protection measures on a device that collects "personally identifying information reflecting the online activities of a natural person."[208] However, that does not assist someone concerned about an intrusive home hub recording her conversations, since the activities are not performed online even if the recordings may be. It could perhaps be argued that whether or not an activity is online through deliberate action by a natural person if it becomes online through a device recording it then it is online. But who would be willing to risk criminal prosecution using that argument as a defense? The IoT tends to collapse distinctions such as online and offline and this demonstrates the unworkability of the narrow exemptions in the DMCA in the face of rapid technological change. Congress was aware that technological developments would render the exemptions in the statute insufficient, so it required the Librarian of Congress to specify narrow exemptions to the crime of circumvention.[209] The Librarian of Congress is thus engaged in delegated rule making. However, each exemption lasts only three years, and will then lapse unless explicitly renewed. While interested parties can argue for exemptions, the Librarian has wide power to refuse to grant or renew an exemption. For example, in 2014, the Librarian refused to renew a provision

[205] Cory Doctorow, DRM Talk at Microsoft, presented at Microsoft Research Group (2004).
[206] Cunard et al., *supra* note 201, at 9.
[207] Randall Roberts, *The Compact Disc Era May Finally Be Entering Its Hospice Stage*, L.A. TIMES, Mar. 2, 2018, https://www.latimes.com/entertainment/music/la-et-ms-compact-discs-20180302-story.html.
[208] 17 U.S.C. § 1201 (i) (1999).
[209] *Id.* § 1201 (a)(1).

that allowed the modification of software that rendered cellphones operable on only one cell phone network.[210] This prevented people moving from one mobile telecommunications network to another. Thus, an unelected official whose typical role was the preservation of books but had been granted additional powers ostensibly to protect copyright, was inhibiting competition in the telecommunications market. The ruling was repealed and replaced by Congress.[211] This demonstrates the unintended consequences of anti-circumvention rules. Anti-circumvention results in a problematic regulatory design of a rule making process in which those requesting exemption must repeatedly demonstrate the need for an exemption or lose the exemption. While law is intended to provide certainty and clarity so that people may plan appropriately the anti-circumvention rule making process generates ongoing uncertainty.

Thus, the aforementioned process is inadequate to meet the new challenges of the IoT. The 2018 exemptions[212] authorize circumvention of controls on computer programs in 'smart televisions' and 'voice assisted devices,' but only to enable interoperability.[213] Controls on computer programs on land vehicles may be circumvented only for "diagnosis, maintenance, or repair," but not for interoperability.[214] Similarly, controls on computer programs in a "smartphone or home appliance or home system, such as a refrigerator, thermostat, HVAC, or electrical system" may be circumvented, but only for "diagnosis, maintenance, or repair." But maintenance and repair are further limited to making a device work according to the manufacturer's original or updated specifications.[215] Many IoT devices fall outside the categories in the exemption, and others are situated within an uncertain grey area. Is a Wi-Fi connected camera a home appliance? Is a device placed in a garden considered a home appliance? What if it is used for security and faces the street? Or if it is used on a farm by someone whose home is on a farm? Even with existing exemptions, it is a criminal offense for the owner of a home hub, that is running proprietary software, that is accompanied by a technical protection measure and is set up to surveil her, to change the software so that it does not send audio or video surveillance data. Ironically, under the DMCA, the owner of the home hub could change the software to prevent it recording which music she plays from an online subscription service but not if it recorded her naked or praying on video. It does not matter whether the owner of an IoT camera or home hub intends to avoid corporate data gathering, to be secure against government surveillance or to protect herself against a stalker or abusive former domestic partner, if she circumvents a technical protection measure to do so she commits a criminal offence. To be clear there is more than one kind of harm at issue here. One kind of harm is an invasion of privacy that occurs when a person is

[210] 77 Fed. Reg. 208 (October 26, 2012) at page 65264.
[211] Unlocking Consumer Choice and Wireless Competition Act, Pub. L. 113-144 (2014).
[212] See background, history and recommendations as well as the final exemptions in 83 Fed. Reg 208 (October 26, 2018).
[213] 37 C.F.R. § 201.40 (7), (8) (2018).
[214] *Id.* at § 201.40 (9).
[215] *Id.* at § 201.40 (10)

actually listened to or watched. Another kind of harm is the erosion of liberty in a society subject to pervasive surveillance. Yet another type of harm stems from anti-circumvention. There are kinds of surveillance which are not unlawful but from which people are free to protect themselves. For example, someone may look from a public street through the window of a room. But the person in the room is free to draw curtains so as to be unobserved. Anti-circumvention prevents people from protecting themselves from surveillance. It is as if the person wishing to draw the curtains found them locked, and if she were to break the lock in order to draw the curtains would find herself charged with a criminal offense.

There is no permissionless innovation for the owner of a thermostat with technical protection measures on its software who wants to tinker with its settings to suit her preferences. The owner of a refrigerator cannot change its software to prevent a known hacking attack unless the manufacturer first changes the specifications. Circumvention of software controls for security research is still criminal, except for research which meets detailed criteria, including that it must not facilitate copyright infringement and must comply with the CFAA.[216] The security researcher whose understanding of any one of these criteria differs with that of a court faces criminal penalties, as does the person whose belief that a Wi-Fi connected garden irrigation system is a home appliance is not shared by the court she is brought before. However, the DMCA with its pinched, provisional arcana is not the most egregious anti-circumvention law. Canadian law also includes anti-circumvention provisions which prohibit circumventing technical protection measures even to do things permitted by copyright exceptions but without any exemptions.[217] While some repair and securing of IoT is sometimes permitted, the net effect is to create uncertainty and risk that inhibits the creation of industry- wide technological standards, or even running sustained consumer education campaigns that address the privacy and security risks of the IoT.

As a result, the owners of IoT devices from thermostats to tractors have lost the right and ability to modify and even repair their own property, except in the most constrained and tenuous ways. The results for the IoT are, as Doctorow observes:

> Today, a startling variety of technologies use digital countermeasures to control their owners: insulin pumps stop you from reading your coronary telemetry except by manufacturer-authorized doctors with paid-up software licenses. GM stops you from visiting independent mechanics who diagnose your engine with unauthorized tools and repair it with third-party replacement parts. Voting machine vendors stop independent researchers from validating their products….designing disobedient computers that view their owners as adversaries, that obfuscate their operations from those owners, that prefer

[216] *Id.* at § 201.40 (11).

[217] Copyright Act, C–42 RSC § 41 (Can. 1985).

> the orders they get from distant third parties to the policies set by the person holding the computer, having paid for it.[218]

It is not just consumers who are at issue. Parents will be unable to prevent essential medical devices from spying on their children. City governments that buy smart traffic lights will find that they do not have full control of such government property, and that public security is compromised as a result. Every solution for addressing the problems of security and privacy for the IoT will have to work around the criminalization of modification and repair.

When IoT devices run free and open source software ('FOSS'), they do not diminish the rights of the owner or operator of the device in the ways that IoT devices running software controlled by EULAs do. FOSS licenses, by their nature, explicitly give permission to modify the software, which alleviates the threat from technical protection measures and anti-circumvention prohibitions. Unlike proprietary EULAs, FOSS licenses tend not to claim rights beyond those in copyright. Some require those who use the software to waive patent claims against others who use the software. Several explicitly remove the anti-circumvention for software under the licenses. Many disclaim liability for use of the software since it is free to use. None of these features of FLOSS licenses reduce the power of owners or users of devices over those devices. In a 2018 survey of IoT developers, 71.8 percent used Linux, a FOSS operating system, for IoT devices.[219] However, there are powerful incentives for manufacturers or other platform controllers to collect personal data through IoT devices. If the power that FOSS gives owners and users over their devices limits data collection there is likely to be a tendency to use proprietary operating systems such as Apple's tvOS[220] or more likely interposing a layer of proprietary software between the user and a FOSS operating system as in Amazon's Fire OS.[221] How can Internet governance leverage the flexibility that FOSS offers for addressing challenges of the IoT?

The criminalization of circumvention is not required by the treaties of the global intellectual property regime. Neither do the treaties require the prohibition of repair or securing by an owner of their property.[222] Although the WCT requires countries to grant a right of rental over

[218] Cory Doctorow, *How Can We Make Technology That Frees Us, Rather Than Enslaves Us?*, TOR/FORGE BLOG (Apr. 3, 2017), https://www.torforgeblog.com/2017/04/03/how-can-we-make-technology-that-frees-us-rather-than-enslaves-us.
[219] Christine Hall, *Survey Shows Linux the Top Operating System for Internet of Things Devices*, IT PRO (May 7, 2018), https://www.itprotoday.com/iot/survey-shows-linux-top-operating-system-internet-things-devices.
[220] tvOS - Apple Developer, https://developer.apple.com/tvos.
[221] Fire OS 5 | Fire OS SDK | Amazon Developer Portal, https://developer.amazon.com/android-fireos.
[222] The provisions of the WCT and TRIPS admit of a number of interpretations, however, no one has yet advanced an interpretation that they actually require laws prohibiting owners repairing or securing their property.

computer programs (Article 7.1),[223] countries need not do so "where the program itself is not the essential object of the rental" (Article 7.2).[224] Thus in international law, IoT devices could be subject to legal rules that specify that a copy of software is sold with the device. However some legal systems, such as the DMCA ignore this flexibility.

TRIPS permits countries to engage in "control of anti-competitive practices in contractual license" Article 40.2 provides:

> Nothing in this Agreement shall prevent Members from specifying in their legislation licensing practices or conditions that may in particular cases constitute an abuse of intellectual property rights having an adverse effect on competition in the relevant market. As provided above, a Member may adopt, consistently with the other provisions of this Agreement, appropriate measures to prevent or control such practices.[225]

This provision has been underutilized, thus its potential power remains untested. As with patents, the global intellectual property regime offers some space for dealing with the consequences of over-reaching licenses and inflated anti-circumvention. Will Internet governance actors make use of this space to make it easier to secure the IoT and keep the data that it generates private? If so, how will non-state actors change the international and national laws which comprise much of the regime?

D. Trade Secrets

Trade secrets are an anomaly in the global intellectual property regime. Treaties on patents were first signed in 1883, and on copyright in 1886. Trade secrets were included for the first time only in TRIPs, signed in 1994. Because trade secrets are mentioned only in TRIPs, they are subject only to the WTO. Strictly speaking, WIPO has no jurisdiction over trade secrets.[226] Trade secrets are dealt with in Article 39 of TRIPS, which reads as follows:

> 2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:
> (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
> (b) has commercial value because it is secret; and

[223] WIPO Copyright Treaty, Art. 7.1, *supra* note 151.

[224] *Id.* at Art. 7.2.

[225] TRIPS AGREEMENT, *supra* note 149, Art. 40.2.

[226] TRIPS does attempt to provide a more venerable lineage for trade secrets in Article 39.1. "In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information. . . ." However since 10bis makes no mention of trade secrets, and the Paris Convention lacks the dispute processes and penalties which apply to TRIPS, this seems no more than a cursory attempt to legitimize inclusion of trade secrets.

> (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[227]

Trade secrets may at first seem unlikely to affect the IoT. Article 39 refers to information without defining it. Information is generally conceived as relating to what humans know and communicate, while computers are described as generating, communicating and analyzing data. While the common meaning of information may change interpretation of the agreement, the term should be understood as it was in 1994 when the agreement was negotiated. It is therefore disputable whether data captured, generated and exchange purely between computers is information for the purposes of TRIPS.[228]

Trade secret law also applies only where information is in fact kept secret through reasonable steps. Artifacts that are widely distributed can be re-engineered and have therefore not been kept secret. Creating or discovering information through re-engineering is legitimate in trade secret law. Trade secret law has historically not been used to prevent imitation of products. Instead copyright, patent and in some jurisdictions registered designs have been deployed to protect things that have been sold and widely distributed. However, this division of labor between different kinds of intellectual property is being undercut by expansive copyright coupled with EULAs and aggrandized anti-circumvention laws that are used to deprive owners of access to the inner workings of their property.

Although technical protection measures may be applied to IoT software, as discussed in Part II , far too many IoT devices, and communications by IoT devices are not secured in other ways. Where this is the case trade secret claims should be refused. Another element required for a trade secret claim is that it be contrary to a judicially ascertained norm. In Article 39 this is articulated as a requirement that information be acquired "in a manner contrary to honest commercial practices." But how can courts ascertain such norms when technology is as novel as the IoT?

In the United States, trade secret law has seen a dramatic expansion and repurposing. As a result a legal remedy intended to encourage commercial parties to disclose information to each other in the course of trade[229] has become a mutable and mutating means for a startling variety of actors

[227] TRIPS AGREEMENT, *supra* note 149, Art. 39.
[228] Robert G. Bone, *The (Still)Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803, 1806 (2014).
[229] Not everyone agrees that there is a coherent policy justification for trade secret law, Robert Bone argues that trade secrets are enforced because of a number of distinct norms borrowed from other branches of the law including contract and privacy. *See* Bone, *supra* note 225.

to sequester information.[230] More than a decade ago, David Levine pointed out a trend toward private provision of public infrastructure coupled with a reliance on trade secret doctrine to prevent the public access to important information about that infrastructure:

> Private businesses are increasingly displacing the government in providing and operating public infrastructure, but these private businesses are utilizing commercial law standards and norms, including the key tool of trade secrecy, to do so. Countless examples of modern infrastructure, from telecommunications in the form of the Internet, to traditional government operations in the form of voting machines, are now being provided by the private sector. Because of this shift to private provision of public infrastructure, the trade secrecy doctrine has intruded into activities that traditionally have been conducted in the relatively open realm of public institutions like government.[231]

Levine points to routers, voting machines, and public Wi-Fi as examples of where trade secrets affect public access to information on infrastructure provided by private actors.[232] It is easy to extrapolate to the IoT; commercial provision of smart traffic lights, cameras, or other public infrastructure could lead to similar conflicts between the commercial interests of private actors and public interests. But if this is a difficult tension to resolve, what of state actors that invoke trade secrets on their own behalf to shield their operation from public scrutiny? San Diego County sought to forestall examination of software used in its voting machines by invoking its own trade secrets in the software.[233] It is easy to extrapolate how trade secret law may be applied to the IoT, for example a city may refuse to disclose data on the operation of city owned smart traffic lights to defendants accused of traffic violations by claiming that they are trade secrets. Levine warns that concealing the workings of public infrastructure through trade secret doctrine will undermine public trust in government.[234] There may of course be good reasons, on occasion, why public actors should be able to maintain secrecy of particular technological details, but those reasons should be articulated so that they can be debated. One response to the problematic deployment of trade secrets in public infrastructure would be for state actors to procure only open source software. By its nature there can be no trade secrets in open source software. Open source software would also resolve the problems of restrictive software licenses and anti-circumvention, since open source copyright licenses explicitly permit modification, and since the source code is available, no technical protection measures apply.

These changes to trade secret law do not automatically change the global intellectual property regime. Attempts to expand trade secrets beyond the purview of Article 39 in individual

[230] David Levine has assiduously researched the development of trade secrets for more than a decade, uncovering the role of trade secrets in public use. The following paragraphs are heavily reliant on his work.

[231] David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 137 (2007).

[232] *Id.* at 177–86.

[233] David Levine, *The People's Trade Secrets*, 18 MICH. TELECOMM. & TECH. L. REV. 61, 96–98 (2011).

[234] *Id.* at 115.

jurisdictions do not formally change the obligations in the Article. However, if the trend of mutating trade law in the United States continues, it will likely lead to efforts to read the mutated doctrine into Article 39 and to incorporate it into future trade agreements. Increasing application of trade secret law to IoT devices severely constrains the policy responses to the challenges of the IoT.

III. Conclusion

The emergence of global Internet governance as a regime that relied very little on legal regulation surprised scholars. Global Internet governance does incorporate law in various ways, but technologies, standards, and standards bodies have proven more central to Internet governance than law. In part, Internet governance developed in this way because of early political decisions in the United States to forgo extensive regulation of the Internet, relying instead on other governance mechanisms. But the discourse of global Internet governance occludes the aporia of intellectual property exceptionalism. As the Internet expanded, and Internet governance became global, the international intellectual property regime reacted to the emerging phenomenon by fashioning new forms of control over digital technology. Internet governance was able to take its non-regulatory form only by skirting the domain of intellectual property. Subsequently, Internet infrastructure, the site of Internet governance, has been co-opted to serve the demands of the intellectual property regime. Imbalance between these regimes served the spread of the Internet as a technology communication dominated by platforms which could either leverage or at least overcome the barriers of surmount intellectual property to take advantage of an otherwise less regulated zone. Internet governance and the global intellectual property regime are fundamentally incongruous. But evidence of the incongruity between the regimes is often explained away, the evidence is framed as pointing only to isolated conflicts which are occasioned by one of the regimes failing to adjust its workings to that of the other, rather than ontological discordance. Consensus on which regime should be adjusted has not always been as easy to find. Consensus should be more easily reached if there are only discrete conflicts rather than fundamental disharmony. But whether a conflict remains unresolved, or has been decided by power rather than principle, it is nonetheless portrayed as resolvable by a purely localized rather than systematic settlement.

As personal data became essential to dominant platforms, the narrative of unsullied technological progress began to fray, inciting calls for new regulation. The eccentric coupling between Internet governance and the global intellectual property regime remains apparently unaffected. This standoff seems unlikely to last. As innumerable, diverse things become connected to the Internet, massively increasingly surveillance and enabling action with physical consequences at a distance, the makeup of the Internet itself is changing. This change, which may be called the Internet of Things, introduces threats to personal and national security, to privacy and autonomy. These issues are prompting national and global policy responses, including demand for new regulations; for example, greater protection of personal data has been implemented in Europe

and may grow in the United States. This, to a degree, undercuts the technological form of Internet governance. As the IoT connects many previously unconnected aspects of life to the Internet, it also potentially increases the reach and importance of Internet governance. Technologies, technical standards, and the bodies that produce them will become even more important for daily life as they determine security, privacy, safety, liability, and the sustainability of many more aspects of human existence. Even efforts to address the challenges of the IoT by regulation will of necessity rely upon technical standards and sometimes technical enforcement through the infrastructure of the Internet.

Whether the response to the IoT is primarily mediated through technologies and standards or through laws, Internet governance is being ineluctably drawn into a decisive engagement with the global intellectual property regime. Intellectual property rules require layers of permission, crippling the potential of permission less innovation. Intellectual property hobbles precautionary approaches. Regulation cannot impose a precautionary duty on a service provider, manufacturer or other actor to secure information, a device or a network connection if that actor is prohibited by intellectual property from making the necessary changes to the technologies involved. Similarly, IoT cannot fail well for as long as anti-circumvention laws put security researchers at constant risk of criminal penalties. The owners of many IoT devices cannot make their own choices about privacy and protect themselves from online attack for as long as anti-circumvention laws threaten them with criminal liability for doing so.

Although this analysis has used the rubric of the Internet of Things as if it consists of a somehow separable network, there is only one Internet, it already includes many things that communicate only with each other, or only with computers that themselves communicate only with other computers. The future of Internet governance is governance of an Internet likely to be comprised by many connected things and relatively fewer connected people. The form that governance takes will in large part be determined by how the current Internet governance regime responds to the policy constraints imposed by the global intellectual property regime.

Will openings in the global intellectual property regime prove useful to responses to the challenges of the Internet of Things? There are some potential openings in the global intellectual property regime, particularly flexibilities in the TRIPS agreement, which allow for the development of legal solutions to patent, anti-circumvention, and trade secret problems. There is some flexibility in the WCT's requirements for anti-circumvention provisions which could be used to avoid the unworkable results of the DMCA and Canadian law discussed although the requirement for anti-circumvention itself persists. But these are openings for legal reform at a national level, or on an international level for treaties or model laws. How can the non-state actors of the Internet governance regime seize these openings? The history of the global intellectual property regime suggests that it is unlikely to exhibit the same kind of lithe reactions as the Internet governance regime.