SIGCIS 2017 Talk

[Opening pleasantries]

[SLIDE: October 21st] On Friday, October 21st, 2016, the Internet went down. **[SLIDE: Dyn map]** Not the whole Internet *itself*, of course, and only for the areas you see on this map, but for those folks many of the major sites that structure our *experience* of the Internet—Twitter, Github, Netflix—all threw up server errors for much of that day. When the dust cleared on Saturday, security researchers placed the blame on an unprecedentedly large distributed denial of service attack, or DDoS. The target: Dyn **[SLIDE: Dyn logo]**, a New-Hampshire headquartered Domain Name System provider. Dyn's one of many companies in this space, which provide the tech through which user-legible domain names translate into machine-legible IP addresses. In other words, this attack affected such wide

swathes of the Internet because it targeted centralized infrastructure, rather than individual sites. But what makes the Dyn attack central to my talk today is not its record scale, but rather *how* it achieved such size. It worked by exploiting vulnerabilities in Internet of Things devices: webcams, smarthubs, toasters. These networked, computationally-enhanced objects, while low-powered, have strength in numbers. And the Mirai botnet, which powered the Dyn attack as well as a number of other record-setting attacks last fall, does just that, aggregating lots of tiny devices into one big wallop. So this is a milestone of sorts: [**SLIDE-D: DJ Roomba**] we have officially entered a reality in which the smart lightbulb you backed on Kickstarter or your klutzy Roomba might in face be weaponized against you.

[**SLIDE-R: Blank**] Today, I offer this weaponization as a way to understand our emerging relationship with these smart objects, and what we construe as the Internet of Things more generally. The Dyn attack is evocative for me because it stages a conflict across two registers: sociability and securitization. [**SLIDE-D: "Sociability"**] "Sociability," an idea I draw from Teodor Mittew, in that it foregrounds the kinds of entanglements in which we find ourselves with these objects both on the level of social life and communication; [**SLIDE-D: "Security"**] "security" in the very real sense that we are made open to attack by and through these objects. What I want to argue today is that these entanglements aren't one-way, but rather *mutual*, that we humans are as sociable with these objects as they are with us or with each other. Moreover, "sociability" might not just be the province of the human, but rather a messy and intimate entanglement of energies across bodies and things. Framing relations like this allows us to consider the Dyn

attack less as a mass deviation—an incursion in a clean network—and more as the amplification of capacities always already latent in the bodies and objects that together constitute the Internet of Things. "Securitization" is then an attempt to regulate these energies. But, as I'll argue, we run up against a technical paradox. As Wendy Chun reminds us, our devices *operate* by promiscuously leaking information: constantly transmitting and receiving signals. I want to extend this to us humans as well. It's then this tension, between the capacity to socialize and leak and how such capacities leave us vulnerable, which is the heart of my paper today. [**SLIDE-R: Blank**]

So let's start with substantiating that first claim: that we are messily entangled with the Internet of Things, and indeed participate fundamentally and equally in it alongside objects. Let's start with the objects themselves.

In its simplest form, an IoT object grafts together a pre-existing technical object, like a mouse trap or a toy doll, and a computer. These computers, for reasons of power and space, are usually quite small and low-powered. They'll often connect to environmental sensors that allow the object to respond dynamically to a variety of factors, like its environment and the operation of other networked devices. These individual nodes are often controlled by smart "hubs," more sophisticated computers that orchestrate all these data flows. And these smart hubs usually displace their interfaces onto one other familiar hybrid: your phone.

So by way of practical example, let me give you one user's description of IoT in action in his own home. This is Arlo Gilbert, writing in 2016 about his Revolv smart hub [**SLIDE-D: Revolv**]:

"I am a home automation nut. When I arrive home my lights turn on. In lieu of motion detecting lights, I have a Z-wave motion detector that notifies my Revolv when there is motion on any side of our home and turns on the appropriate lights. Although I do set a home alarm, there is really no more effective vacation security than the programatic turning on, dimming, and turning off of lights in a manner that would indicate that people are home. After buying my Revolv I put my outdoor landscaping light on it and threw away the old timer. Now at Sunset my landscape lighting turns on. Holiday lighting does the same. It's magical."

Sounds like EPCOT, right? (Parenthetically, some of you may know this piece because Gilbert wrote it in a rage after Google announced it had bought out and was shutting down Revolv's servers, effectively turning his smart hub into a,

quote, "container of hummus." The question of control always lurks just outside of the frame.)

[**SLIDE-D: Gilbert's text**] Gilbert's dream is a good example of the promises that IoT makes for our lives. I draw our attention to the play of light here, which responds to movement and time. [**SLIDE-D: Highlight #1**] This play, moreso than anything else in the passage, creates friendly, livable, and safe domestic space. [**SLIDE-D: Highlight #2**] And not only can Gilbert's home respond to motion or time, but through *light* it can appear to simulate someone living there even when no one's home. This is the dream of IoT self-sufficiency: a system that can function independently, inscribing the human body as a negative space, perceptible and reconstructable as the sum of a body's *traces* on the space. To use the EPCOT frame again, the human becomes a kind of *special effect*.

[**SLIDE-R: Blank**] We are all acutely aware of the traces that we leave on the Internet and the negative images Facebook and the NSA can construct of us. The Internet of Things, I contend, applies these principles to a particularly *fleshly* register: bodies become data. But it's a flesh that is also curiously *devoid* of flesh, as we see in Gilbert's home simulating human presence. One lightbulb responds to another, which might pick up communication from a thermometer in a garden gnome, which all ominously bend to a Russian botnet. There are two levels of legibility at work here, which, following the recent work of philosopher Yuk Hui, I contend are the *technical* and the *digital. Technical*, in that these objects are legible within a discourse of tool-making familiar to philosophical discourse through Simondon and Heidegger; and *digital* in that these objects also exist as structured data objects—similar to an email or a piece of xml. The Internet of Things stages a definite collapse between these categories both on the level of being

and on the level of communicative acts. Smart objects are *technical* in the sense of being tools and *digital* in that they exist as concrete nodes on a network. Moreover, they *act* by producing and responding to digital objects—data—of all kinds. This dichotomy, which is also a synthesis, begins to get mapped onto bodies. To a lightbulb, I'm not *that* materially different from a fellow lightbulb. This is the blurring of imagined categorical boundaries.

[**SLIDE-D: Internet of Assemblages**] So instead of a clean, spare, addressable network, we have a fleshly, volumetric, constantly-reorganizing assemblage—language through which I want to defer both to Deleuze and Guattari and to Donna Haraway's ideas of the cyborg. Such a framing, particularly that of the cyborg, helps us begin to see the sensory capacities of computationally-enhanced objects as actually *decoupled* from computation as such. In this claim I draw on Kari Kraus's work on what she calls "enchanted

things," a different term for computer-thing hybrids. She observes that physical objects "are already lo-fi sensors in the natural state," for example, a book that grows moldy in response to humidity, or that records waxy traces if read by candlelight. With the frame of the Deleuzian assemblage, it makes sense to then talk about the "sociable" work of the Internet of Things as marshaling productive capacities, energies that are not necessarily human or object or computer, but rather emerge from and flow along channels of material specificity and political possibility. I call these acts "sociable" to do two things: 1) to highlight how, through the addition of computation, we are making *legible* in objects communicative capacities that we previously imagined to be just the province of humanity, [**SLIDE-D: Point #1**] and 2) to *decouple* these capacities from the realm of the human, and to begin to articulate how "sociability" manifests differently across human and object. [**SLIDE-D: Point #2**] The computer becomes a tool through which these

capacities are intensified and channeled in certain ways. Such a move then allows us to ask why, in the presence of such objects, we humans *begin* to behave like data, make ourselves *legible* as objects: it's a different, though related, kind of "sociability."

So now I come back to the Mirai botnet and the Dyn attack thinking through this legibility and the vulnerabilities therein.

[**SLIDE-R: Mirai**] The word "mirai" is, ominously, Japanese for "future." After the wave of attacks last fall, its source code was posted GitHub [**SLIDE-D: Github**], so we can see that it's actually pretty crude code in the end. A compromised device operates normally but continuously scans the public Internet for a range of IP addresses corresponding to other Iot devices. Once it finds a target, it uses a dictionary attack of the sixty-two most common default usernames and

passwords for IoT devices to break through. [**SLIDE-D: Usernames and passwords**] Its operation is kind of basal-level sociability, the purest ideology of the Internet of Things. Both on the level of technics—one thing pinging another thing—but also on the level of construction, in that its operation depends on the flawed work of end-users who never change their passwords or manufacturers who never give users that opportunity. So in a way, these tactics are not categorically *different* than normal operations. This is an attack of *excess* and *purity*, of *unmanaged* energy, rather than something qualitatively new and different.

(I then frame "security" as the work of tactically managing this excess so that these energies don't boil up and over into mass DDoS attacks. And I mean "dangerous" really honestly here. At a recent hearing before Congress, Bruce Scheier warned that DDoS attacks—which are, again, at root just a basic act of networked connectivity taken up to eleven—could feasibly

target other networked infrastructures, like hospitals. Elevators. Ventilation systems. I dug up a report from last November from a town in Finland in which a DDoS attack turned off an IoT-automated heating system in the middle of winter. This shit's real.)

[**SLIDE-R: Blank**] So in this frame, I want to return to Wendy Chun's arguments that I mentioned briefly at the top of this talk. In her recent work on networks and habituation, she argues that at the most fundamental level, [**SLIDE-D: Slogan**] our networks work by "leaking." While we may think that our wireless network cards are just identifying available local networks, for instance, they are in fact constantly scanning, writing, and deleting all packets in range—all signals, all noise. "Promiscuity," or sociability, is central, not peripheral, to how our devices work *with* each other. Implicit in her argument is how, in getting to entangled with our fleshy lives and imbricated in our human

sociality, the Internet of Things begins to make legible how *we* are also communicating by leaking. This is of course the central idea behind tracked advertising, such as the famous incident a few years back when Target could accurately predict whether or not a woman would become pregnant through her online purchasing habits.

It's all too easy to lay the blame at end-user's feet here, for "consenting" to such tracking, or for not taking their passwords seriously. Indeed, such a framing emerged at that same congressional hearing I mentioned earlier, in which Kevin Fu, a professor of computer science at the University of Michigan, argued for a "significant change in cyber hygiene," without which IoT cannot be considered secure. He was arguing for governmental oversight of critical Internet infrastructures, which is certainly practical, but I note that the turn towards "hygiene" [**SLIDE-D: Wirecutter article**] situates the human being as a kind of final weak link

in a chain of security. Doing so makes sense in the short term, but misconstrues, I think, what we're framing as insecure. It's not the human that's insecure, but rather, as I've tried to argue, *vectored sociable energies* that can emerge from human and object alike. Without such a framing, we can't begin to understand or embrace situations in which "openness" or "vulnerability" can be anything other than dangerous. The challenge I offer is to understand sociability and vulnerability in IoT as productive spaces: terrain open for the formation of solidarities, rather than an ever-interior turn towards the "local" as the single body or home.

[**SLIDE-R: Final**] I would reconfigure the Internet of Things as an Assemblage of Sociable Energies (it's not as catchy, I know), one in which we are mutually interdependent with objects that indeed *can* make our lives more interesting, joyous, practical or impractical. In such a frame, *security*, insofar as it is the useful managing of tactical vulnerability

rather than the delimitation of energetic possibility, must arise from both human and nonhuman agents. If our devices operate through insecurity, then they must be open to vectors through which attacks can occur. As I've argued, that Mirai targets insecure usernames and passwords reveals the human agent itself as a part of the security apparatus. Insecurity then moves both ways, as devices leave humans open to attack while humans leave devices open to attack. I think the chill in that sentence emerges more from our prevailing cultures of securitization, which outwardly demonize the sociable even as they demand it for operation. Of course, control can't help but enter the frame: if we had platform cooperatives rather than centralized megacorps, this would probably be a very different talk. But for now, we are caught between the rock and hard place of sociability and securitization. I'm not going to stick the dialectical landing here, but in such moments I want to turn back to Donna Haraway's relentlessly call for a material and political

embrace of our "joint kinship" with technology, our partiality and hybridity, our mutual introjection and prosthesis. Our devices operate by leaking and so do we: not only tracing out smells, secretions, rhythms, habits, and movements, but also by recognizing and responding to the traces of others. In this Assemblage of Sociable Energies, the human is a useful but not a special category; and "security" is the practice of kinship rather than isolation. This is an optimistic image, I know. It has no immediate answers for malicious actors, *(aside from keeping your heating system off the goddamn Internet to begin with)*. But I hope it begins to map territory for imagining a more capacious "we," along lines of technology and humanity alike.