Disinformation gets physical: The internet of things as an emerging terrain

By Laura DeNardis

I can live, and live abundantly, as a digital human being who has never been on Facebook or Instagram. But I can't live, work, or socialize without the underlying systems of technical architecture and governance that keep the internet operational and connect the cyber-physical world around me. The institutions that operate this infrastructure include cloud computing providers, internet registrars and registries, transaction and financial intermediaries, network operators, hosting companies, DNS resolutions providers, certificate authorities, and Internet of Things (IOT) system operators, to name just a few categories. They are not immediately visible to end users in the same way content and applications are visible. Yet they are the internet's most powerful control points.

Understanding both vexing disinformation problems and powerful solutions to these problems requires a deeper dive beneath social media into underlying infrastructure points of control and the companies that operate at these various layers. As I have written about in the past (e.g., here, here, and here), the internet's core infrastructure provides choke points — for better or worse — at which content and transactions can be blocked, altered, or co-opted. The Indian government's approach to shutting down the internet or China's approach to censorship and control exemplify how internet architecture is a now proxy for geopolitical power, as well as every manner of content control from DNS-based copyright enforcement to cloud computing-based filtering of child pornography. During the rise of COVID-19 disinformation, web hosting company Squarespace took down the website of the so-called America's Frontline Doctors organization for violating its terms of service by making spurious claims such as not needing masks to battle COVID-19.

As more things than people are now connected to the internet, what is less obvious is how the internet diffusing into the material world all around us — the so-called internet of things — connects to disinformation. Far more "things" than people connect to the internet. These objects — whether Wi-Fi connected medical devices, consumer IOT, industrial cyber-physical systems, or smart city infrastructure — exist simultaneously in both the material and cyberworld.

In my new book, "The Internet in Everything: Freedom and Security in a World with No Off Switch," I note that "all of the policy issues in two-dimensional digital space have leapt into three-dimensional real-world space and have added new concerns around physical safety and everyday human activity." The internet of things has not yet been drawn into policy debates about disinformation, and this should change. The IOT is an emerging terrain of disinformation, and possibly one that is more consequential than social media influence campaigns, computational propaganda, video deepfakes, or any manipulation involving human content and communications. The following are three broad categories of disinformation arising via the co-option of IOT infrastructure:

The IOT as an ex-ante source of disinformation

The United States emerged from a contentious 2020 presidential election rife with unsupported accusations about fraud and corrupt voting machines. The increasing politicization and weaponization of election infrastructure raises an important question that transcends both the computational influence campaigns of 2016 and the far-fetched accusations of election fraud of 2020: How could an election be disrupted via internet of things disinformation?

As I suggest in The Internet of Things Could be an Unseen Threat to Elections, this type of disruption is technically and politically feasible, and even easy. Rather than hacking directly into voter rolls or the election apparatus, disrupting an election would merely require disruptions to energy, transportation, home alarm, or weather systems that depend on IOT sensors, in order to dissuade or distract people from voting in areas that are either heavily Democratic or Republican. False traffic jams or false forecasts of inclement weather can suppress the vote on election day, for example. As an “artist” in Berlin demonstrated, creating a false traffic jam does not even require hacking into traffic systems, but simply rolling a wagon filled with cell phones down a street to simulate a traffic jam and turn a Google Maps street red.

The global pandemic has helped remind society that the internet of things is also the internet of self, and a critical part of socially distanced medical care. Cyber-connected medical devices include wireless cardiac appliances, insulin pumps, telemedicine diagnostic equipment, and other objects adjacent to or embedded directly in the flesh. Hospitals and medical facilities are notoriously targets of ransomware attacks that lock up information systems until a Bitcoin payment is made to a hacker. But so too are consumer medical devices vulnerable to attack, creating an entirely new terrain of disinformation that, instead of creating political and social tension, can create a life or death medical problem.

Transductive attacks — deepfakes on steroids

What is a “deepfake” in the IOT? Because IOT devices coexist both in the real world and the digital world, hacking is as much about physical world manipulation as a digital attack. This transforms the scope of cybersecurity from a digital problem to both a digital and material problem. The IOT fundamentally relies on a process that can be called "transduction," the conversion of one form of energy to another. For example, a sensor detects a signal in the real world (e.g., motion, rotation, sound, temperature, or pressure) and converts that to a digital signal that is then authenticated, processed, and even encrypted in a way that legitimizes the integrity and validity of the data being collected. Then the inverse occurs. The cyber-physical system converts the digital signal into a physical signal in which an actuator *acts* on something, such as unlocking a door, opening a pipeline valve, or turning off a light.

This transduction brings about many social and economic benefits, such as detecting and addressing a leak in a pipeline. But it also creates a new point of vulnerability for surveillance, manipulation, disinformation, and attacks generally. Some of these are straightforward "born-digital" manipulations, such as installing intentionally faulty car emissions sensors to generate fake emissions data.

But rather than simply attacking or manipulating cyberspace directly, it is now only necessary to change something in the physical world, such as a temperature, which is then "sensed," digitized, and used to provide information such as climate change data, only carrying the imprimatur of highly legitimized and authoritative data because the system authenticates and verifies the digital data without knowing that the real-world signal was manipulated. The deepfake risk is no longer about hacking or digital manipulation but about manipulating the real-world data that then feeds into a digital system. Cybersecurity — and the detection of deepfakes — is therefore as much about mechanical engineering and fluid dynamics as information engineering.

The IOT as an amplifier of human disinformation

The IOT also makes disinformation and disruption originating in the screen-mediated human internet far more potent. The intimate data collected about people via connected appliances, cars, or medical devices is easily weaponized, such as making phishing attacks or a manipulative email more credible. As just one example, receiving an email with accurate information gleaned from a connected object makes the manipulation more believable and makes the recipient more likely to click on the malicious link or share fake information. The suppression of true information is also part of disinformation. DDoS attacks carried out by hijacked cyber-physical objects mute content by flooding the site with false requests. The security and integrity of information on a legitimate content site — whether a media or political campaign site — is only as secure as the security of the IOT. Indeed, one of the largest DDoS attacks in history — the Mirai Botnet — attacked major social media and content sites using hijacked IOT devices. The IOT is not only a threat matrix, but also an emerging threat plane from which to disrupt legitimate information and amplify disinformation.

The political case for securing the IOT

Importantly, note that stronger IOT security could thwart all three of these cyber-physical disinformation entanglements. Despite the extraordinary societal dependency on internet-connected physical infrastructure, and despite the consequences of these infrastructures for privacy, human safety, and national security, the IOT is still notoriously insecure. Addressing the democracy and human safety implications of disinformation now requires taking into account the internet's diffusion into the biological and material world and the security of the internet in everything. The internet is in objects that are both cyber and physical, making cybersecurity a great human rights issue of our time. As the internet moves from 2D into 3D, we have to expect that so too will disinformation — and disinformation policy — move from 2D to 3D.

Laura DeNardis is a professor at American University, a Yale ISP Affiliated Fellow, and the author of "The Internet in Everything: Freedom and Security in a World with No Off Switch" and other books. She served as executive director of the Yale Information Society Project from 2008 to 2011.