The world needs tighter IoT governance. But reforms are on the way.

Cybersecurity and privacy protections are missing for much of IoT. A slew of new international standards and laws promise to change that.

It's been a wild three months in the world of IoT cybersecurity. Researchers from Unit 42 recently discovered, for example, that criminal botnets had attempted to worm their way into hundreds of millions of smart devices afflicted with the CVE-2021-35394 vulnerability from August to December last year. Before that, there was a warning from Microsoft that hackers were using a discontinued web server still commonly accessed by security cameras and software development kits. And, we mustn't forget the scandal of Roomba customers discovering screenshots of their homes being posted on Facebook – an incident arising from an AI training program for these devices that many users have since complained they were never fully aware was happening.

It's a state of affairs that unnerves Madeline Carr – one that she believes has largely come about because of a total lack of consensus among legislators about how IoT devices should be properly secured. A professor of global politics and cyber security at University College London, Carr recently co-authored an essay for the World Economic Forum arguing for much tighter legal governance regimes for IoT. For most of the world, she explains, there simply aren't any rules or regulations directly governing how an IoT device should be secured against hacking or privacy violations, effectively leaving it up to companies in the space to decide for themselves how to protect consumers.

Many are still uninterested in, or lack the capacity to fully comprehend, the problem, argues Carr. "Lots of manufacturers simply have little or no understanding of the implications of the product they're producing," she says. Take your average smart doorbell. "You don't know what context that will be used in – and, so, you don't know what level of security it might need or might not need."

Companies that do take an active interest, meanwhile, are often relying on a patchwork of international standards like ETSI EN 303 645 or ISO 27404, which provide a guide to maintaining the interoperability and security of their device (and how not to fall foul of most privacy legislation), but still remain mostly voluntary. These documents, says Carr, "are just ways for manufacturers and service providers to say, 'Okay, if I do my thing this way, it will be interoperable, or it'll be most likely regarded as safe or appropriate.'"

That's great if every single consumer and company can agree on the exact interpretation of what is and isn't appropriate for cybersecurity and privacy in IoT devices. In most cases, however, they can't, which naturally leads to strange and troubling variations in the levels of protection built into individual products and legal absurdities arising from laws never designed to cope with the challenges thrown up by IoT. Tesla vehicles, for example, come equipped with a cornucopia of sensors and cameras powering its 'Sentry Mode' – so many, in fact, that the Bavarian Data Protection Authority said owners who used that option should be considered fully-fledged data controllers under the EU's GDPR.

Then there are the more obvious cybersecurity risks that arise from disagreement over governance standards. Recent years have seen myriad cases of IoT devices being forcibly recruited into criminal botnets, helping to facilitate DDoS attacks and ransomware offensives. As our dependency as a society increases on IoT, so too will our vulnerability to cyberattacks at an increasingly large and destructive scale.

"We're basically building porosity into our critical information infrastructure by embedding millions of unsecured mobile devices into our built and natural environments," says Carr. "And there's simply not going to be any way to go back and retrieve those devices once they've been proven to be problematic."

Reforming IoT governance, one law at a time

Fortunately, reform is on the way – and, in the case of the UK, here already. Last month, the Product Security and Telecommunications Infrastructure (PSTI) Act became law. The legislation compels all firms that manufacture, import or distribute IoT devices to comply with stringent new security requirements. The law also forces companies to investigate, act on and maintain a record of all cybersecurity failures, and to prevent the distribution of insecure products. Consciously imitating the penalties demanded by those firms violating the EU's GDPR, non-compliance with the PSTI Act invites a fine of £10m or 4% of worldwide revenue. The law will officially come into force with at least 12 months' notice to allow businesses to prepare (although the specific regulations underpinning the law have yet to be published.)

The UK isn't alone in this regard. The EU, for example, is in the process of enacting its Cyber Resilience Act, envisioning even tighter cybersecurity protections for consumers using IoT devices. The US, too, has proposed new regulations in this area. Formulated by officials from the White House National Security Council, the Biden administration's labelling initiative would see all IoT devices clearly explain security information relevant to the product through the use of a simple labelling system. A QR code would also be included to allow curious consumers to delve into the weeds about how best their smart fridge might be insulated against cybercriminal gangs.

Such progress on IoT governance cannot be allowed to stall, says Carr. What's at stake is the future of a technology that, at its core, promises to make life better, safer and in some cases longer for its users. But people need to trust in it – and that can only come with a concerted effort to agree on basic rules governing cybersecurity and privacy for IoT devices as soon as they are manufactured. A good example of the kind of balance that can be struck between IoT functionality and safety, says Carr, can be found in the ecosystem that supports financial transactions across the internet. "Those sectors know that if ever people lose confidence in online banking, that would be catastrophic to their business model," she says.

What's more, getting there shouldn't require an international conference of all interested stakeholders. "It's not necessarily about everyone having the same law or international agreement about what our laws should be," says Carr, but advancing consensus around IoT governance gradually, for the safety of all. "It's about inching the landscape forward, bit by bit."