

Dr. Cory Doctorow (h.c.)
3727 W Magnolia Blvd
Burbank, California
USA 91505



27 January 2022

To: Mr. A. Hermans,

Portfolio Committee on Trade and Industry, Parliament

For attention: Mr A. Hermans, Ms M. Sheldon, Ms. Y. Manakaza, Mr. T. Madima, via email: ahermans@parliament.gov.za ; tmadima@parliament.gov.za; msheldon@parliament.gov.za; and ymanakaza@parliament.gov.za

Dear Committee,

Re: Submission on Copyright Amendment Bill – January 2022

I write today in relation to proposed amendments to the regulation of Technological Protection Measures in Sections 1 and 28O of the Copyright Amendment Bill.

I am an internationally recognised expert on TPMs, and have participated in WIPO treaty negotiations relating to them, as well as standardisation efforts at the World Wide Web Consortium, Digital Video Broadcasters' Forum, Broadcast Protection Discussion Group, OASIS and elsewhere. I hold an honorary doctorate in Computer Science from the Open University (UK), where I am a Visiting Professor of Computer Science; I am also a Visiting Professor of Practice at the University of North Carolina School of Library and Information Science; and a Research Fellow at the MIT Media Lab. I serve as a Special Advisor to the US Electronic Frontier Foundation, an organisation I have been associated with for 20 years. I am also the author of more than 20 books, many of them *New York Times* bestsellers that have been translated into dozens of languages, and am thus familiar with questions related to copyright, fairness and the arts.

I note with alarm that the Copyright Amendment Bill's TPM provisions have moved closer to the US regime defined in Sec 1201 of the 1998 Digital Millennium Copyright Act (hereafter "DMCA 1201"). It's impossible to overstate the extent to which DMCA 1201's defects have made it a locus of real mischief in the US, and how these defects are apt to impose even higher cost on South Africans.

The Original Sin: Failure to Require a Nexus With Infringement

DMCA 1201 was putatively enacted in order to satisfy America's obligations under the WIPO Copyright Treaty (WCT) and the WIPO Performers and Phonograms Treaty (WPPT) (collectively known as "The Internet Treaties"). These treaties require member states to prohibit the use of circumvention devices **from being used to aid in copyright infringements**.

However, the US implementation did not take account of the nuance in the WIPO treaties. Rather the US enacted a blanket prohibition on tools capable of circumventing any system that served as an access control (TPM) to a copyrighted work. This was no minor oversight, rather, it was a charter for corporations to write their own private laws and outsource their enforcement to the nation's criminal justice system.

By failing to require a nexus with infringement, DMCA 1201 ushered in an era in which any manufacturer could conjure up new felonies in relation to their products, reaching beyond the point of sale to criminalise conduct by competitors, critics and customers that was not optimal for their shareholders.

Under normal circumstances, a person who purchases a product is free to use it in any way they see fit. The manufacturer of your shoes cannot force you to buy your shoelaces from them as well. Your dishwasher's manufacturer cannot reach out from beyond the point of sale to dictate which dishes you can load into it.

The freedom conferred by ownership carries over to ancillary services and the merchants who provide them. The company that sells you a kitchen knife can't force you to bring it to their authorised knife-sharpening depots to pay a premium for "sharpening services" and they certainly can't dictate to you when your knife is beyond sharpening and order you to trade it in for a new one at significant cost.

We take these freedoms for granted. Likewise, we take for granted the principle that consumer advocates, academic researchers, independent reviewers and other third parties are free to examine the products we might buy and warn us if they contain significant defects.

However, all three of these freedoms – the freedom to arrange our conduct to our own benefit rather than that of the shareholders of the companies whose products we purchase; the freedom of third parties to offer accessories, consumables, services and repair for the products we own; and the freedom of auditors to uncover and publicise defects in the products we rely on – are all compromised by DMCA 1201.

Any device that contains software embodies a "copyrighted work." A manufacturer who places a minimal TPM on such a device transforms it into a "covered device" for the purposes of DMCA 1201 enforcement. The plummeting cost of microcontrollers (notwithstanding the current, transient price spikes brought on by pandemic-related supply-chain disruptions) has made it tractable to transform the most unlikely and mundane gadget into a "covered device." Commodity system-on-a-chip (SoC) components add pennies to the bill of materials for a new product, and now it is common to find TPMs not just on phones or cars or refrigerators – but also on car engine parts, phone screens, even the charcoal filters fitted to new refrigerators.

This allows the manufacturer to exercise tremendous control over devices long after they have been sold:

- Medtronic, the largest med-tech company in the world, uses TPMs to prevent hospital technicians from repairing broken ventilators; [this practice continued even after pandemic travel restrictions grounded all of Medtronic's authorised technicians, just as demand for ventilators was spiking](#);
- [HP and other printer vendors use TPMs to lock out third-party ink cartridges and to enforce "regionalisation" of ink](#) (blocking ink purchased in one country from being used in another),

as well as unilateral best-before dates. These TPMs are sometimes altered through deceptive software updates that are disguised as "security updates"

- Apple uses TPMs to block third-party app stores on the phones it sells to its customers; [Apple's own store extracts high surcharges from app vendors, who pass this along to Apple's customers](#). Apple also uses its veto over which apps can run on its customers phones to exclude apps that compete with its own services.
- [Security researchers are often chilled by DMCA 1201 claims](#); manufacturers that deploy a TPM can threaten security researchers with criminal sanction if they disclose defects in their products, on the grounds that these disclosures threaten the integrity of their TPMs.

As embedded systems proliferate, so do TPMs. Firms can and do design their products so that their TPMs must be bypassed in order to use those products in ways the manufacturer disfavors. Because bypassing a TPM carries a criminal sanction, this allows firms to literally criminalise conduct that displeases them, without any legislature ever banning that conduct. As Cydia creator Jay Freeman puts it, this is "felony contempt of business model."

It's Worse For Africa

As bad as this is in wealthy nations of the global north, it's far worse in an African context, thanks to the gap between the experiences of users in the global south and the experiences of the technologists, designers and product managers in America and China who have the final say in how dominant tech platforms' tools will work.

When the person designing your digital tools lives in a radically different built environment, speaks a different language, comes from a different culture, is unfamiliar with your faith traditions, works under a completely different political system, shares few or none of your dietary preferences, and enjoys a material standard of living (including reliable infrastructure and utility services) unlike your own, that person is bound to create tools that are not fully suited to your purposes.

The fact that users in the global south have needs that are poorly met by digital tools, multiplied by the fact that those users are badly situated to convince tech giants to change those tools, creates a strong case for interoperability without seeking permission from distant American or Chinese tech giants.

The motto of the accessibility movement is "nothing about us without us": it's a demand that the users of systems, services and products be included in their design and management. This ethos is not the sole purview of people with disabilities - everyone who's ever had a tool imposed on them without their guidance or consent intuitively understands that they know their needs better than anyone.

The movement for inclusion in tech boardrooms has made important strides in developing products and services that are more thoughtful about users' needs, but *a priori* determinations of those needs will always run up against the limits of our ability to predict all the ways that they will change in the real world.

Technology has an answer for this unknowable variable future: rather than design tools so that they can manage every contingency out of the box, we adapt them to our circumstances. Sometimes, we reconfigure them (say, by turning on closed captioning so we can enjoy a streaming video when our Bluetooth headphones' battery dies) and sometimes we alter them (as when a medical technician

repairs a ventilator with a broken screen by swapping in a screen from a broken ventilator with a working screen).

Reconfiguration and adaptation are important everywhere, but nowhere moreso than the global south, where western assumptions about the supply of parts, reliability of internet and mains power, and the need to extend the duty-cycle of devices are wildly disconnected from the conditions on the ground.

This is where interoperability comes in, and it is common practise in the global South, ingenious ways of making technologies work. *Jugaad* may be an Indian phenomenon, but every part of the global south - and every place the world over where people have to mend and make do - there are equivalents, for example, *jua kali* (Swahili), *gambiarra* (Brazilian Portuguese) and *bricolage* (France and its former colonies).

All of these words refer to a form of interoperability without permission: the imaginative reconfiguration of diverse components to adapt or repair a system to suit local needs and conditions.

As US and Chinese Big Tech companies have vied to turn “the next billion users” into captives of their locked-in silos, clever engineers and toolsmiths have assisted their neighbors to adapt to local conditions the hardware and software that wealthy empires push over their borders.

Take GBWhatsApp, an app with truly global provenance. It has its origins in conflict-torn Syria, where free/open source developers created an alternative client to plug into Facebook’s massive WhatsApp messaging service. Its core is a software library, libwhatsapp, that is maintained by a global community, playing a cat-and-mouse game with Facebook engineers who seek to break compatibility between these unofficial clients and the main network.

Though GBWhatsApp users can be found all over the world, they are most concentrated in Africa, where the unofficial WhatsApp client is also a *de facto* standard. Africa is obviously not a monolith: with 1.2 billion residents in 54 countries, the spectrum of African use-cases is broad indeed. Accordingly, GBWhatsApp has exploded into a whole constellation of variants, each adapted further to some niche where it fits perfectly.

These variants sport enhanced privacy features (like the ability to turn off “read-receipts” asymmetrically - so that you can see when conversation partners read messages, but not the other way around) as well as expanded support for local dual-SIM phones, allowing a user to log in to more than one WhatsApp account from a single device.

As GBWhatsApp demonstrates, interoperability without permission is the means by which local toolsmiths can create a locally appropriate technology without having to do so from whole cloth. Rather, they can build atop of, or alongside of, other technologies from elsewhere. The false choice of “local” or “global” is thus revealed: the global tool can take on local characteristics and form a blend of both: bricolage, or if you prefer, *jua kali*.

A TPM regime that does not tie a prohibition on circumvention to copyright infringement is a death-sentence for Made-in-South-Africa technological innovation – it is an invitation to foreign giants to usurp the role of the South African Parliament in deciding what is and is not permissible in respect of the digital technologies and ICTs that South Africans depend upon and relocate that authority to the boardrooms of Silicon Valley and Shenzhen.

The Proposed Amendments Make the Copyright Amendment Bill Worse

The current draft of the Bill erases the protections for non-infringing circumvention that were latent in the original text:

- Changing the definition of TPMs to include those that restrict lawful uses as well as infringing uses.

A tool that accomplishes a lawful purpose should be lawful. The WCT and WPPT do not seek to limit activities that displease corporate rightsholders; they only seek to thwart copyright infringement.

- Importing DMCA 1201's prohibition on tools "with a limited commercially significant purpose or use other than to circumvent a technological protection measure."

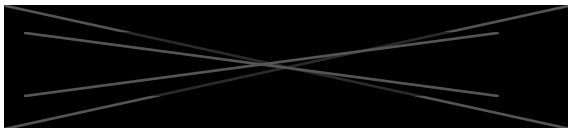
Free/open source tools often have *no* "commercially significant purpose." This language endangers some of the most successful and popular free/open tools, tools like VLC, that are in wide use in South Africa today for everyday technology users, archivists, educators, and creators.

- Making "negligence" the standard for culpability under the ban on circumvention tools, rather than "intent."

This is the kind of broad language that is guaranteed to chill the production of general-purpose tools that might incidentally also constitute circumvention devices, something that is especially risky in the field of security research, where it would implicate debuggers, decompilers, and other essential tools for security audits.

Advisors to the South African Parliament have argued that these extreme, over-reaching prohibitions on circumvention and tools must be integrated into South African law to satisfy its treaty obligations. This is categorically untrue: the WCT and WPPT do not require that South Africa follow America's ill-starred experiment in giving corporations the power to create private law and wield it against its citizenry.

Sincerely,



Dr. Cory Doctorow (h.c.)