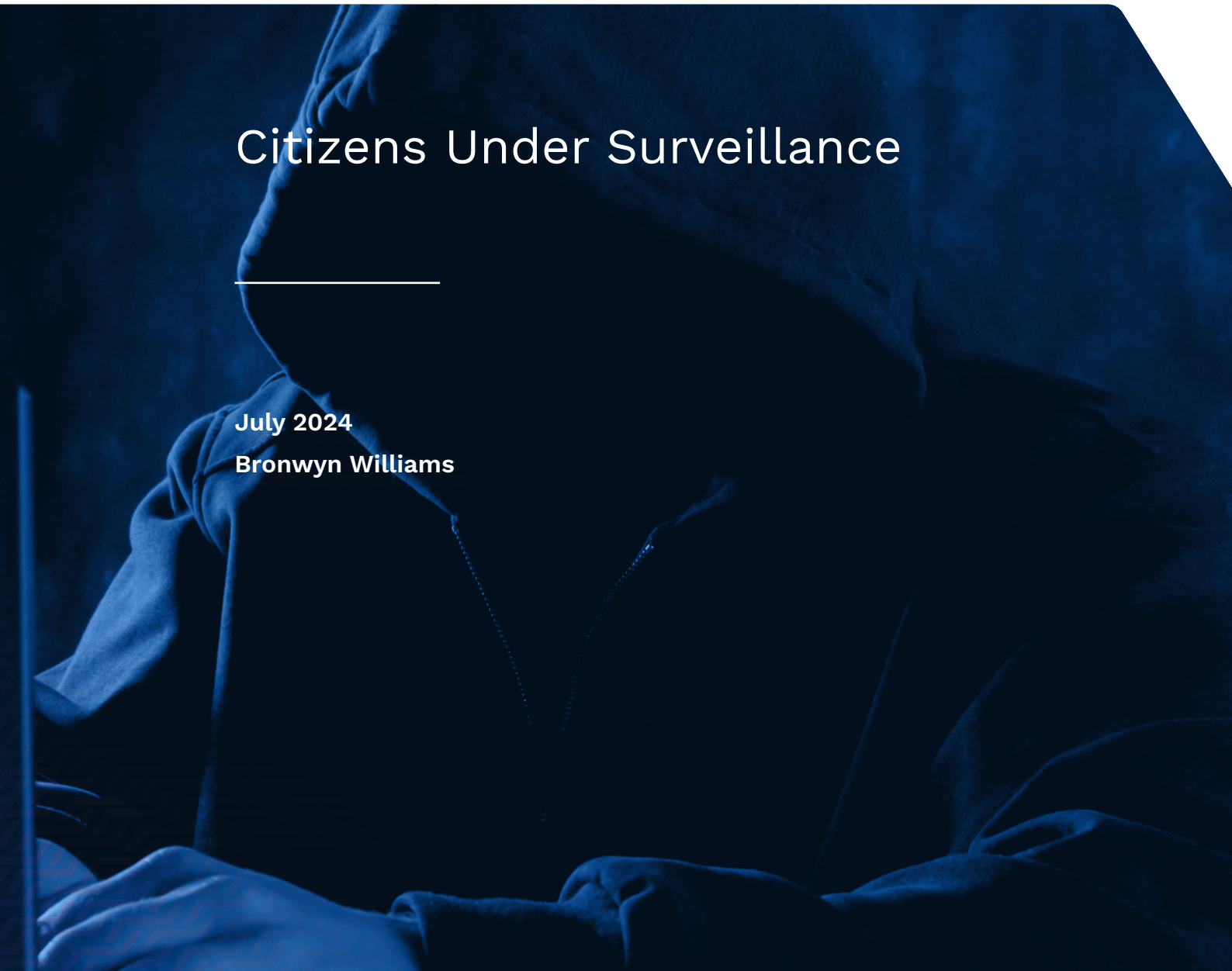
REPORT

IRR

Online risks and harms



Citizens Under Surveillance

July 2024

Bronwyn Williams

Table of Contents

July 2024

Published by the South African Institute of Race Relations

222 Smit Street (Virtual office),
Braamfontein Johannesburg, 2000, South Africa
PO Box 291722, Melville, Johannesburg, 2109, South Africa
Telephone: (011) 482–7221

Author: **Bronwyn Williams**

Editor: **Terence Corrigan**

Typesetting: **Mbali Mayisela**

Cover image: **Unsplash/Bermix Studio**

Online Safety Laws and the Risk of 'Open Air Prisons' If We Continue Conflating Risk with Harm

Not with a bang but with a whimper, the democratic world is moving, one bill at a time, from objective rule of law to subjective rule *by* law.

A new spate of global and local mass digital surveillance bills targeting 'online harms' are being drafted into law across the Western world in the name of protecting the public in general, and children in particular, from risk of harm. This has potentially vast implications for personal liberty and privacy.

The open-ended, multi-purpose 'skeleton key' laws being passed in supposedly liberal democracies can be used to monitor, censor, punish, and criminalise almost anyone at will. Of particular concern is the way these new laws attempt to criminalise subjective, poorly defined harms such as 'offence' or 'effect on mental health' – or, even worse, the risk of harm.

This conflation of risk with harm becomes particularly apparent when we apply this logic to our increasingly digitised and virtualised lives, as many of the new harm and safety bills do. As such, it is worth considering how our contemporary society is being virtualised in two different ways.

First, in the literal sense, more and more of our experience is being digitised. The continuous is increasingly being made discrete. What is digitised and discrete can be codified, flattened, and managed into 'computer says no/go' algorithmically imposed rules which allow us to 'govern' the ungovernable through increasingly sophisticated, increasingly automated bureaucracies.

Second, in the more figurative sense, we have become virtualised in the sense of our becoming untethered from reality as we deny objective truth (or even the possibility thereof) in favour of the unfalsifiable subjective 'lived experience'.

These two trends are not in conflict, despite first impressions. Rather, they represent a feedback loop – whereby reality is denied and deconstructed and then progressively replaced by a new set of rules and laws that serve as an enforced proxy of a new 'consensus reality' defined by binary bits and bytes.

To see how this plays out in the political sphere to manufacture and secure power, Arlyn Culwick remarks:[1]

> '*Virtualisation* is Western bureaucracy's principal means to gain power — and to bring ruination upon the whole society. Virtualisation in this context is —
> Step 1: commodify mere possibilities (i.e. risks) instead of just actualities.
> Step 2: identify more risks and market them to the population. Expand power.
> Step 3: the market economy becomes oriented around unrealities — mere possibilities. Its terminus is thus unreal.'

In other words, in a virtualised society, there is no limit to the loophole opened by John Stuart Mill's Harm Principle, which suggests that the actions of individuals should only be limited to prevent harm to other individuals.

If harm can be convincingly redefined as risk, there can be virtually no legitimate limits to power employed in the pursuit of risk mitigation. After all, risk is infinitely elastic, especially when it comes to any narrative involving potential harm to children (and here, any suggestion of pornographic exploitation in particular) or any threat to national security (or, more specifically, the spectre of terrorism). As such, it is very difficult to argue against risk mitigation measures, however small the associated risk is in reality.

A good example of the subtlety at play here is the UK's new Online Safety Act, that allows for jailing people who cause others 'likely psychological harm', which is, rather obviously, highly subjective. According to *The Times,* the law, which went into effect in February 2024, 'will shift the focus on to the "harmful effect" of a message rather than if it contains "indecent" or "grossly offensive" content, which is the present basis for assessing its criminality.'[2] (Similar bills are being proposed across the world and are outlined in the following section.)

As such, the bill, and those like it, become effective skeleton keys that can be used to lock just about anyone you don't like away, by claiming just about anything they said (or posted online years ago when the zeitgeist was a bit more tolerant of diversity of opinion) caused you 'likely psychological harm'.

After all, how can you prove that you did not cause someone psychological harm with your words? Or that your comments did not influence 'national values' which could in some way affect 'national security'?

More importantly, if harm can be re-defined in terms of subjective claims such as psychological instead of physical safety rather than objective truths, or, indeed, if subjective claims to harm can be codified into discrete punishable crimes, claims to legitimate power can be manufactured at will. Power becomes as infinitely elastic as the war on risk.

South Africa's amendments to RICA and the newly introduced GILAB legislation should be viewed in the same light: as an attempt to conflate risk with harm to justify gross violations of human rights, particularly those relating to privacy, dignity, and freedom of speech.

An overview of the global landscape of emerging mass digital surveillance bills

> *'These governments' underlying belief is that democratic countries committed to the rule of law shouldn't be stymied by technologies like encryption. But they have it backward: any government that infringes on the right to privacy of its populace cannot claim the democratic high ground. Democracy, of course, is not just about strong rule of law. Democracy also requires checks and balances on the most sensitive and frightening aspects of governmental power, including surveillance. And because of its covert nature, surveillance can so easily be abused without checks and balances.'*
>
> - Mallory Knodel, CDT's Chief Technology Officer, member of the Internet Architecture Board and the co-chair of the Human Rights Protocol Considerations research group of the Internet Research Task Force.

South Africa is not alone in its trajectory. It is notable that subjectively defined digital mass surveillance bills are being simultaneously rolled out across the Western democratic world. In general, these new-generation bills justify mass surveillance, censorship, and attacks on the right to private (encrypted) speech by promising to reduce the risk of harm to children. That said, the new digital harms and safety bills build on the logic and precedents set by previous spates of mass surveillance justification following the 9/11 terrorism attacks, which promised to protect civilians from national security threats if they submitted to curtailment of their rights to privacy and freedom of movement.

United Kingdom: Online Safety Act, 2022[3]

'Is an algorithm going to be able to reliably tell the difference between someone encouraging suicide and someone with postnatal depression posting about feeling suicidal on Mumsnet?'

- Mark Johnson, Big Brother Watch[4]

In theory, UK's Online Safety Act promises to 'deliver the government's manifesto commitment to make the UK the safest place in the world to be online while defending free expression'.

In practice, the law, which went into effect in February 2024, will require tech platforms and social networks to 'protect' their users from vacuously defined online 'harms' – or run the risk of fines of up to 10% of the firm's global revenues. With such sums at stake, businesses are heavily incentivised to both censor and surveil their users on behalf of the government.

Censorship will likely err on the side of caution, and due to the scale of the businesses in question, likely rely on algorithmic drag nets (mass surveillance of all content posted on these platforms) and enforcement, which could easily result in both false positives and false negatives.

Furthermore, due to the law's focus on 'children', tech platforms will be pushed to verify the ages of their users, which will effectively end anonymity online, as age verification presently requires some form of identification. (Although web3 self-sovereign digital identity schemes could go some way to resolve these the issue of anonymity, they are not currently in place at scale).

Meta, Google, and X are already pushing such voluntary verified identity schemes in anticipation of these laws.[5]

Furthermore, not satisfied with tech platforms policing their own users, the law also includes provisions for the British government to use 'accredited' technology to preemptively scan all citizens' digital messages across all platforms and messaging channels as a preventive form of 'safety', effectively ending the legal use of end-to-end encryption, and, therefore, effectively treating all citizens as guilty until proven innocent, regardless of credible suspicion of criminal activity.[6]

European Union: Digital Services Act, 2023 (DSA)[7]

The law regulates online intermediaries and platforms with the aim of preventing illegal and harmful activities online. The law also promises to prevent the spread of 'disinformation' (again, like 'risk of harm', impossible to define clearly in practice).

As with the UK's online harms law, the Digital Services Act requires platforms to be responsible for monitoring and controlling illegal content posted or shared on their services. Again, complying with the law's sweeping mandates will encourage, if not necessitate, tech platforms to surveil and censor user communications.[8]

European Union: Regulation Proposal on Child Sexual Abuse Material, 2022 (CSAM)[9]

'The problem is that it's very easy to break the hash by changing one pixel or even by slightly cropping the image. It's also possible for a perfectly legitimate image to be flagged as a false positive.'

- Bart Preneel, a cryptography expert at KU Leuven University[10]

The Regulation Proposal on Child Sexual Abuse Material aims to prevent and combat online child sexual abuse and lays out clear obligations for service providers to 'detect, report, remove and block access to online child sexual abuse material'.

Again, if the regulation is approved, platforms platforms will be required to enforce effective end-to-end encryption. The regulation recommends that platforms run perceptual hash functions, which would effectively compare the digital fingerprints (or hashes) of known and identified harmful digital content (for example explicit content involving minors, or perhaps 'hate speech') to all files shared across the platform's network.

The hash comparisons would be required to check for matches to illegal content in users' locally stored files in addition to files sent and shared via the platforms' messaging services, which, obviously, would require a violation of users' privacy.

The proposed regulation is a perfect example of the difficult choice between doing everything possible to protect children on one hand, and the innocent majority's right to privacy and freedom of expression on the other.

'This regulation would have safeguards, Europe is a democracy, not a dictatorship. And let's not be naive: in a dictatorship, when you want to spy on citizens you do spy on citizens. You don't need a new regulation.'

- Mié Kohiyama, co-founder of the Brave Movement and advocate for more regulation.[11]

As could be inferred from the above quote, proponents of the bill are fully aware that the regulation will effectively amount to legalising 'spying' on its citizens.

USA: Kids Online Safety Act, 2023 (KOSA)[12]

If approved, the Kids Online Safety Act will require social media platforms to put the interests of children first by requiring platforms to make safety the default and to give kids and parents tools to help prevent the destructive impact of social media.[13]

The bill is yet another example of using children as human shields to shoehorn increased surveillance and censorship regulation and undermine the right of individuals to anonymity online. As with European legislation, the American version makes technology businesses and platforms responsible for 'preventing and mitigating' a range of potential risks of harm to minors, ranging from depression, anxiety, addictions, and eating disorders through to bullying, harassment, and sexual exploitation. Again, the generous wording of the bill, and the potential penalties for failing to prevent the wide-ranging possible harms, will push platforms to adopt age (identity) verification as well as mass censorship and surveillance measures.

'Ultimately, this puts platforms that serve young people in an impossible situation: without clear guidance regarding what sort of design or content might lead to these harms, they would likely censor any discussions that could make them liable.'

- Electronic Freedom Foundation[14]

USA: EARN-IT Act, 2020[15]

The EARN-IT Act sets requirements for both the government and interactive computer service providers (such as Internet providers and social media companies) to use technological means to monitor and report online exploitation of children.

In effect, the law requires suspicion-less scans of every online message, photo, and hosted file, again effectively subjecting every citizen to a perpetual digital police search without the requirement of a search warrant.[16]

The EARN-IT Act proposes client-side (on device) scanning of data for prohibited content and as such will require cooperation from the likes of Apple as well as from online platform companies.[17]

Australia: Online Safety Act, 2021[18]

The Online Safety Act aims to improve and promote online safety for Australians.

While fairly innocuous in itself, the act also requires the tech industry to develop new – legally enforceable – codes to regulate illegal 'harmful' and restricted content for children and adults. The codes, which are still being negotiated between government and industry, will likely result in similar legislation to that which is being developed in Europe and the USA, requiring age and identify verification for users, and a responsibility to surveil and censor content deemed harmful.

Australia: Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA), 2018[19]

The Telecommunications and Other Legislation Amendment Act updates regulation around government access to telecommunications, computer access warrants and search warrants.

In effect, the law empowers the government to force technology companies and platforms to circumvent encryption and allows the government access to intercept and monitor user data and communications.

The cost to the economy in terms of lost trust and consumer confidence as a direct result of the law is estimated to have already exceeded a billion Australian dollars.[20]

Canada: Bill C-63[21] , 2024

Canada's Online Harms Act, formally called Bill C-63 (before the Canadian House of Commons in early 2024), is perhaps the most concerning of all. Like the other bills discussed, this bill is proposed to prevent online harms in general, and terrorism and child exploitation in particular. In addition, the bill promises to protect the population from 'scam ads' and non-consensual creation and sharing of deep fake pornography created using citizens' likenesses.

However, the penalties proposed for violating the law are nothing short of extraordinary. The bill makes provision for courts and judges to hand down life sentences for hate speech violations relating to the promotion of genocide, and up to five-year jail terms for other online hate crimes.

It should also be noted that the legislation seeks to redefine the concept of hatred itself, to include 'the content of a communication that expresses detestation or vilification of an individual or group of individuals on the basis of prohibited grounds of discrimination'.[22] Grounds for discrimination in this context include 'race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics, disability or conviction for an offence for which a pardon has been granted where a record suspension has been ordered'.

Furthermore, the bill contains provision for a new class of 'peace bond' (a peace bond is similar to protection orders granted in other countries). The new peace bonds will allow judges to 'impose conditions on an individual where there are reasonable grounds to fear that they will commit a hate propaganda offence or hate crime, such as where there are reasonable grounds to fear that someone will willfully or intentionally promote hatred against an identifiable group. As this is a preventative measure to protect all people in Canada, there would not be the need for evidence that an offence has actually been committed'.[23]

This essentially means that people could be placed under house arrest, and compelled to wear ankle monitors or other tracking devices on mere suspicion that they could commit a hate (or more, specifically defined "discrimination") crime in the future. No hate crime, let alone any actual physical crime would have to be committed for the punishment and restrictions to be enforced.

This becomes particularly concerning, given that the bill encourages and empowers individuals or 'groups' who have felt offended to report future hate crime suspects to the government; individuals or 'groups', of course, that could have personal vendettas against the individuals they chose to report under this broad sweeping bill that effectively convicts and contains individual liberty on mere suspicion and without the right of trial.

Public-private protection partnerships – Big Brother in bed with Big Business

In summary, the synchronised online harms and safety bills mean private sector platform companies have responsibilities in the eyes of the law that may be at odds with the interests and rights of their customers.

Companies that offer cloud-based solutions can be prosecuted and punished for hosting illegal content on behalf of us, their users. They can also be pushed to co-operate with law enforcement when it comes to ongoing investigations.

To avoid prosecution, and to protect and advance their business interests, the big platform-based businesses that form the backbone of our digital lives will co-operate with governments and the law, undermining promises of encryption and privacy, and allowing state actors access to the personal information we have entrusted them with.

Effectively, all consumers – and citizens – are now assumed guilty until proven innocent. (And, yes, these international laws will affect foreign citizens too, as platform companies and ecosystems transcend national borders.)

The system of wholesale scanning of phones to search for a reason to suspect someone is guilty can be viewed as the digital equivalent of policemen performing routine daily searches of the homes of everyone living in an entire country just in case someone is harbouring something suspicious. This should be contrasted with the current usual legal system which at least nominally presumes citizens' innocence until proven guilty and requires law enforcement investigators to obtain a warrant to search a person's home or devices based on a reasonably justified suspicion of guilt.

While such measures may be well intended, private companies preemptively partnering with law enforcement opens up a whole world of possibilities for abuse by less than benevolent authorities. For example, the same image-hash matching software that can be used to spot and prosecute child abusers could also be repurposed to spot and persecute activists harbouring whatever content their authoritarian governments don't like.

'Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent... The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding.'

- US Supreme Court Justice Louis Brandeis

South African Surveillance

South Africa: General Intelligence Laws Amendment Bill, 2023 (GILAB)[24]

'National security means the measures, activities and the capabilities of the State to pursue, advance [sic] any opportunity or potential opportunity and the security of the Republic and its people including national interests and national values as contemplated in section 198 of the Constitution.'

- GILAB Bill

The General Intelligence Laws Amendment Bill is a sweeping piece of proposed legislation that redefines national security as well as the government's roles and rights in upholding it. The bill also removes many of the restrictions that currently limit the government's legal ability spy on its own citizens and grants wide-ranging discretionary powers to the government minister appointed to control the South African Intelligence Agency envisaged in the bill, and tasked with implementing it.

As with the international skeleton key laws discussed earlier, changing definitions of words and phrases from the specific to the more general can be used to broaden the depth and breadth of government surveillance in almost any direction desired to infiltrate and intercept practically any aspect of civic life the government desires to keep tabs on.

'The Bill expands the legal definitions of key terms, including "domestic intelligence", "foreign intelligence", "intelligence gathering", "national security", "national security intelligence", and "threats to national security". These changes significantly broaden the mandate and powers of South Africa's intelligence structures, including to proactively seek any "opportunity or potential opportunity" to advance South Africa's national security interests.'

- Intelwatch[25]

Furthermore, the bill is worded in such a way that it would allow government intelligence services to 'gather, correlate, evaluate, and analyse' domestic intelligence on 'any internal threat or opportunity or potential opportunity or threat or potential threat to national security' to 'identify and impede any threat or potential threat to the security of the Republic and its people'.[26]

The Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA)[27]

'Today technology enables law enforcement agencies to . . . invade the "intimate personal sphere" of people's lives, but also to maintain and cement its presence there, continuously gathering, retaining and – where deemed necessary – using information.'

- Constitutional Court

The original RICA law of 2002 governed the interception of communications in South Africa.

In many ways, RICA was a preview, or a slightly more analogue version, of the new-generation digital anti-encryption bills now being adopted across the Western democratic world. Among other provisions, the bill made encrypted telecommunication services (that is telecommunications that do not have the capability to be intercepted) illegal in South Africa – along with the right to anonymous telecommunications, by mandating identity verification of SIM cards and private company record keeping of clients' personal information and communications, the very same rights in principle currently under attack by global digital regulations.

However, although the bill makes provision for lawful interception and therefore legalised some forms of government surveillance and record keeping, it also made provision for the protection of personal rights though specific limitations on the government's reach over personal information and privacy. In theory at least, the right to privacy in general remained protected by our Constitution.

More recently, in 2023, the theoretical rights to privacy outlined in both RICA and the South African Constitution were put to the test in a Constitutional Court case brought by AmaBhungane against the government for intelligence overreach and unjustified mass surveillance.

In a landmark ruling, the Court found RICA incompatible with the South African Constitution in terms of both the right to privacy and the rights to dignity and freedom of expression, and by extension, the 'interconnected rights' to assembly, freedom of association and the right to make political choices. It gave Parliament an opportunity to review and amend the act to make it compatible with the law of the land.[28]

The Constitutional Court found that although RICA made no provision for mass surveillance of private communications of the public, the law failed to make provisions for differentiation between intimate and personal communications, relevant and irrelevant information and innocent vs implicated individuals. In addition, the Court found that the government had been involved with 'unlawful and invalid' mass surveillance through bulk key-phrase scanning, 'interception of all internet traffic that enters or leaves South Africa, including the most personal information such as emails, video calls, location and browsing history'.

Many of these gross violations have been justified by the so-called 'section 205 loophole' found in section 205 of the Criminal Procedure Act. This law makes provision for police and government investigators to seize call, internet, or just about any other communications records after obtaining a magistrate's order, which is not subject to any of the safeguards provisioned in RICA.

Following the Constitutional Court case, it was hoped that the amended RICA bill would address the Section 205 contradiction and reinforce citizens' rights to privacy. However, the draft amendments fail to close the loophole and do little to strengthen citizens' rights in any material way. Furthermore, the GILAB bill only further undermines the constitutional mandate for privacy, dignity and freedom of speech and association, pointing to a larger trend towards greater government surveillance.[29]

Future implications of South Africa's mass surveillance strategy

'The more you know the more frightened you are.'

- Ropeik, Gray, 2002[30]

It is interesting to note the Constitutional Court's focus on dignity as the nexus between anonymity, freedom of speech, and freedom of association, or the lack thereof, when it comes to issues of state surveillance and personal privacy.

These rights will only be further conflated as technology begins to enable us to intercept not only our digital communications, but even our very thoughts. Neuro-rights, 'cognitive ergonomics', or the right to privacy of thought (or lack thereof) are already topics up for debate at the UN and the World Economic Forum.[31]

The stakes around the precedents set by our tolerance of digital interception are deep and far reaching. The interest we take in challenging new overreaches by the government into our personal privacy and freedom of speech and association not only at the polls, but also, where warranted, at the Constitutional Court level, will have a clear and profound impact on our future human rights.

In the more immediate future, GILAB's empowerment of the government to peek deep into the activities of NGOs, opposition parties, and the media requires urgent attention, as any attempts to silence or spook legitimate opposition to government behaviour should be seen as a direct attack on democracy. The intense subjectivity and broad language of the laws and draft legislation in question should likewise be seen as an attempt to further the back-door accumulation of power via skeleton key laws that can open and shut at will – a slippery slope from rule of law to rule by decree.

Likewise, laws like RICA that deny the innocent the right to anonymity along with the guilty and refuse us the right to opt out of being flattened and tracked and digitised in order to be 'seen' and studied by the state should be challenged. Online and off, anonymity allows whistleblowers, political refugees, dissidents, and politically unfavourable voices the cover and protection they need to speak up.

Similarly, anti-encryption regulation threatens the right and freedom of journalists, abuse victims, human rights activists, opposition politicians, and even lovers, to speak and love freely.

We should not fall into the trap of conflating risk with harm to justify these gross violations of personal rights to dignity – to the dignity at least of being considered innocent until found guilty enough to be served with a search warrant.

It is all too easy to believe that no preventative measure or intrusion into our daily lives is too great a sacrifice to prevent even the possibility of harm, be that a risk of child exploitation or a risk to national security. However, that line of thinking forgets that much of what passes for preventative security is more security theatre than security.

The term 'security theatre' was coined by Bruce Schneier, a Fellow at Harvard University's Berkman Center, to explain the difference between security measures that increase actual security and security measures that have an effect on our belief about how secure we are without actually changing our level of risk.

We would do well to understand the difference when it comes to accepting greater and greater levels of government scrutiny of our personal and online lives in the name of 'security'. Yes, security is a tradeoff between freedoms. But we should question whether we are getting any more actual security in exchange for the vast range of rights and freedoms we are being asked to curtail.[32]

‘We must guard against the acquisition of unwarranted influence, whether sought or unsought.’
- President Dwight Eisenhower

At the very least we should demand transparency around the surveillance of our private communications, as the UN Commission for Human Rights, the Tshwane Principles on National Security,[33] and the South African Constitutional Court all validate. This means that we should reject or challenge any vagaries in tone, language and intent to ensure legislation cannot be used as a skeleton key law by unscrupulous politicians.

Furthermore, as civil society, we should demand evidence that any curtailment of our rights and freedoms is, as the United Nations General Assembly mandates, ‘consistent with the principles of legality, necessity and proportionality’.

Lastly, and perhaps most importantly, however, we should also look to ourselves. As Sam Roggeveen wrote in an essay looking back at the aftermath of 9/11 and ahead at the seemingly inevitable march towards greater and greater surveillance:

‘The short answer is that governments are eroding our civil liberties because we asked them to. We are the ones who elected and re-elected governments that vastly increased the size and reach of domestic intelligence agencies. And we are the ones who have meekly acquiesced to the costly, time-consuming, irritating, and almost entirely pointless security theatre that makes our airports such a nightmare. What signals have we, as a people, ever sent our governments that we think they are overdoing it? When have we ever told our politicians that it is politically safe to ratchet down their descriptions of the threat? What have we done to ensure that politicians won’t be labeled “soft on terrorism” if they propose to reverse some of the excesses of the last decade?’

Perhaps it is time to send some signals at the polls and in our courts, and to remind ourselves, and our governments, who works for whom.

Endnotes

1. Interview with Arlyn Culwick, 24 February 2020.
2. Dathan, M, 2021, 'Trolls will be jailed for "psychological harm"', *The Times*, November https://www.thetimes.co.uk/article/trolls-will-be-jailed-for-psychological-harm-2dccb2cct
3. Government of the United Kingdom, undated, Supporting documentation for legislation to establish a new regulatory framework to tackle harmful content online, and make reforms to the criminal law. https://www.gov.uk/government/publications/online-safety-bill-supporting-documents
4. Big Brother Watch Team, 'The Economist – The Online Safety Bill Could Change The Internet As We Know It', Big Brother Watch, May 25. https://bigbrotherwatch.org.uk/2022/05/the-economist-the-online-safety-bill-could-change-the-internet-as-we-know-it/
5. *The Economist,* 2022, 'Britain's Online Safety Bill could change the face of the internet', *The Economist,* May 25. https://www.economist.com/britain/2022/05/25/britains-online-safety-bill-could-change-the-face-of-the-internet; Article 19, 'UK: Online Safety Bill is a serious threat to human rights online', Article 19, April 25. https://www.article19.org/resources/uk-online-safety-bill-serious-threat-to-human-rights-online/
6. Big Brother Warch Team, 2023, 'Five Things you need to know about the Online Safety Bill', Big Brother Watch, October 3. https://bigbrotherwatch.org.uk/2023/10/five-things-you-need-to-know-about-the-online-safety-bill/
7. European Commission, undated, The Digital Services Act. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
8. Galaski, J., 2022, 'What is the EU Digital Services Act? What are its Main Goals?', Liberty. EU, July 5. https://www.liberties.eu/en/stories/digital-services-act/44360
9. Council of Europe, 2022. European Commission: Regulation Proposal on Child Sexual Abuse Material (CSAM), Council of Europe, May. https://www.coe.int/en/web/cyberviolence/-/european-commission-regulation-proposal-on-csam
10. Jones, M.G., 2023, Planned EU laws on child sexual abuse have sparked a bitter privacy row. Why?, MSM October 19. https://www.msn.com/en-za/news/other/planned-eu-laws-on-child-sexual-abuse-have-sparked-a-bitter-privacy-row-why/ar-AA1ivgDb
11. Jones, M.G., 2023, Planned EU laws on child sexual abuse have sparked a bitter privacy row. Why?, MSM October 19. https://www.msn.com/en-za/news/other/planned-eu-laws-on-child-sexual-abuse-have-sparked-a-bitter-privacy-row-why/ar-AA1ivgDb
12. Congress of the United States, A Bill to Protect the Safety of Children on the Internet, 118th Congress, 1st session, 2023. https://www.blackburn.senate.gov/services/files/D89FC49B-0714-4124-B8B1-4F35A85F5E02
13. Blumenthal, R., and Blackburn, M., undated, The Kids Online Safety Act of 2022. One-page information sheet. https://www.blumenthal.senate.gov/imo/media/doc/kids_online_safety_act_-_one_pager.pdf

14. Kelley, J., 2023, 'The Kids Online Safety Act is Still a Huge Danger to Our Rights Online', Electronic Freedom Foundation, May 2. https://www.eff.org/deeplinks/2023/05/kids-online-safety-act-still-huge-danger-our-rights-online
15. United States, 2020, EARN IT Act of 2020, 116th Congress, https://www.congress.gov/bill/116th-congress/senate-bill/3398/text
16. McKinney, I., 2023, 'Dangerous EARN IT Bill Advances Out of Committee, but Several Senators Offer Objections', Electronic Freedom Foundation, May 10. https://www.eff.org/deeplinks/2023/05/dangerous-earn-it-bill-advances-out-committee-several-senators-offer-objections
17. American Civil Liberties Union and Center for Democracy & Technology, 2015 Secret Surveillance: *Five Large-Scale Global Programs,* Submission to the United Nations Twenty-Second Session of the Universal Periodic Review Working Group Human Rights Council. https://cdt.org/wp-content/uploads/2014/09/cdt-aclu-upr-9152014.pdf
18. Government of Australia, Online Safety Act, No. 76 of 2021. https://www.legislation.gov.au/C2021A00076/latest/text
19. Government of Australia, Telecommunications and Other Legislation Amendment (Assistance and Access) Act, No 18 of 2018. https://www.legislation.gov.au/C2018A00148/latest/text
20. Olshansky, S., and Wilton, R., 2021, 'How Do Surveillance Laws Impact the Economy?', Internet Society, June 1. https://www.internetsociety.org/blog/2021/06/how-do-surveillance-laws-impact-the-economy/
21. First Session, Forty-fourth Parliament, 70-71 Elizabeth II – 1-2 Charles III, 2021-2022-2023-2024, House of Commons Canada, Bill C-63. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading
22. Government of Canada, February 26, 2024. https://www.canada.ca/en/canadian-heritage/news/2024/02/backgrounder--government-of-canada-introduces-legislation-to-combat-harmful-content-online-including-the-sexual-exploitation-of-children.html
23. Government of Canada, February 26, 2024. https://www.canada.ca/en/canadian-heritage/news/2024/02/backgrounder--government-of-canada-introduces-legislation-to-combat-harmful-content-online-including-the-sexual-exploitation-of-children.html
24. Government of the Republic of South Africa, 2023, General Intelligence Laws Amendment Bill, B40-2023. https://www.parliament.gov.za/storage/app/media/Bills/2023/B40_2023_General_Intelligence_Laws_Bill/B40_2023_General_Intelligence_Laws_Bill.pdf
25. Intelwatch, 2023. *Briefing Note: General Intelligence Laws Amendment Bill (GILAB),* Intelwatch, November 17. https://intelwatch.org.za/2023/11/17/briefing-note-general-intelligence-laws-amendment-bill-gilab/
26. De Bos, P., 2023, 'New Intelligence Bill is Anti-Democratic, and a Unique Mix of Malice and Stupidity', Daily Maverick, September 7. https://www.dailymaverick.co.za/article/2023-09-07-new-intelligence-bill-is-a-unique-mix-of-malice-and-stupidity/

27. Regulation of Interception of Communications and Provision of Communication-related Information, Act 70 of 2002. https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13
28. Kruyer, C., and Chambers, T., 2023, *Reforming Communication Surveillance in South Africa Recommendations in the wake of the AmaBhungane Judgment and Beyond,* Intelwatch and the Media Policy and Democracy Project. https://intelwatch.org.za/wp-content/uploads/2023/05/Intelwatch_Reforming_communication_surveillance_in_South_Africa_May_2023.pdf
29. Intelwatch, 2023, 'RICA Bill misses the Chance for Real Reform', Intelwatch, September 20. https://intelwatch.org.za/2023/09/20/rica-bill-misses-the-chance-for-real-reform/
30. Kalfoglou, S., 2019, 'Aviation Security: Illusion of Safety or Reality?' *Lectio Socialis,* 3(1), pp. 1-8.
31. Hickman, H., 2015, 'Could Mind Reading become a Reality?', World Economic Forum, November 26. https://www.weforum.org/agenda/2015/11/could-mind-reading-become-a-reality/
32. See Anderson, R., 2020, *Security Engineering: A Guide to Building Dependable Distributed Systems* (Third Edition). Indianapolis: John Wiley & Sons Inc.
33. Open Society Justice Initiative, 2013, *The Tshwane Principles on National Security and the Right to Information: An Overview in 15 Points.* https://www.justiceinitiative.org/publications/tshwane-principles-national-security-and-right-information-overview-15-points#:~:text=June%202013-,The%20Tshwane%20Principles%20on%20National%20Security%20and%20the%20Right%20to,and%20national%20law%20and%20practices

IRR

South African Institute of Race Relations

www.irr.org.za

info@irr.org.za

(011) 482 7221