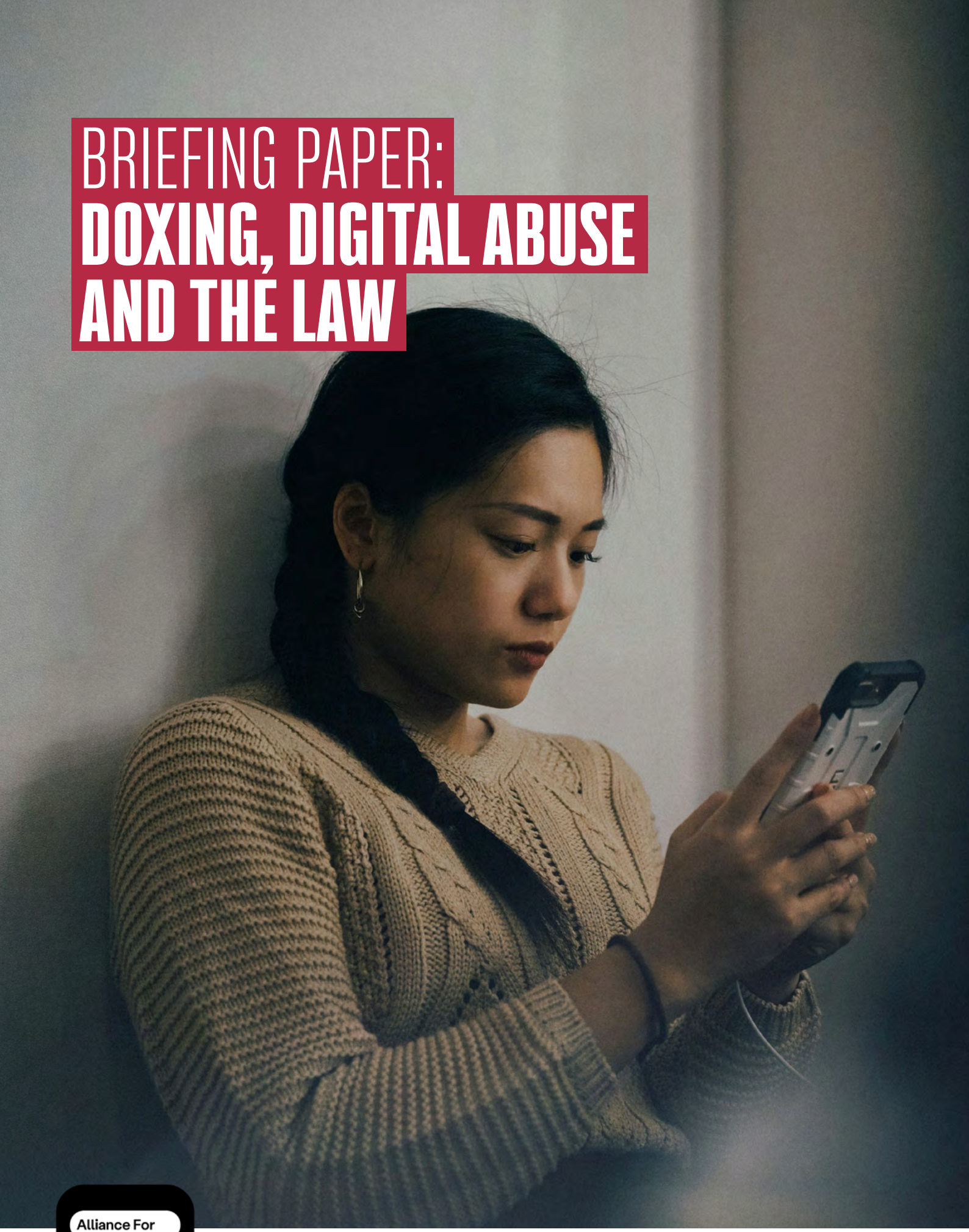
BRIEFING PAPER:
DOXING, DIGITAL ABUSE AND THE LAW



Alliance For Universal Digital Rights

Equality Now
A just world for women and girls.

CONTENTS

This factsheet was written by, and reflects the views of, Equality Now, following research done on a pro bono basis by Hogan Lovells International LLP. The underlying research that informed the factsheets was concluded in September 2023 and has not been updated. The factsheet is for information only. It is not intended to create, and receipt of it does not constitute, a lawyer-client relationship with Hogan Lovells International LLP.

OVERVIEW

This brief provides preliminary research findings on the legal frameworks in nine focus jurisdictions designed to protect people from doxing, a form of online harassment. To understand what legal protections exist, with pro-bono support from a law firm, we researched laws in England and Wales, Scotland, Australia, New Zealand, South Africa, Kenya, Nigeria, the US (Virginia, Texas, California), the European Union, and international human rights law. The research considered what laws are currently regulating doxing. It also looked at prospective laws, soft laws, and other areas of law, such as copyright, defamation, and consumer law.

In releasing this brief, we aim to enable discussions among diverse stakeholders on the legal approaches required to address doxing effectively.

Our research found no definition of "doxing" in international human rights law and no international human rights laws that directly regulate or tackle "doxing".

Also, across the different jurisdictions, we did not find a law that specifically referenced the term 'doxing', but we found two laws that make it a criminal offence to share another's personal information. In the US state of Texas, the Texas legislature passed a bill in 2023 that made it unlawful to disclose a residential address or phone number under the Texas Penal Code. It is a state law and, therefore, only applies in Texas.

In France, Article 223-1 of the Criminal Code[1] prohibits revealing personal information when such an act enables that person to be identified or located with the intention of exposing them or their family to a direct risk of harm.

Other countries have a variety of laws that could, in theory, be applied to tackle doxing.

In Australia, doxing could be regulated under the Criminal Code Act. In the UK, several laws might provide some redress, such as the Protection from Harassment Act and the Malicious Communications Act. And victims of doxing might be able to get posts containing their personal information taken down under the UK's new Online Safety Act.
Doxing may be unlawful in Kenya under the Constitution and the Data Protection Act. Similarly, protection against doxing might fall under the right to privacy under the Constitution of Nigeria. In South Africa, a person may be deemed to have committed an offence of doxing under the Cybercrimes Act or the Protection of Personal Information Act.

The European Union does not have a specific law on doxing, but it could fall under the GDPR and a proposed Directive on combatting violence against women and domestic violence. In New Zealand, the offence will likely fall under the Harmful Digital Communications Act.

For the US, in California, the California Penal Code criminalises the release of personal information, and the Virginia Code in the US state of Virginia might provide for a similar offence.

Evidently, there is not a consistent approach across different legal jurisdictions for a victim of doxing to seek help having their personal details removed from online platforms or to seek redress from harm caused. In some countries, a patchwork of several laws might apply, including criminal offences and civil remedies. This makes it likely that action to seek remedies would be neither fast nor easy.

1 Article 4 Criminal Code (France)https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043974282

INTRODUCTION

'Doxing' (or 'doxxing') is a form of online harassment that refers to the searching and sharing of private information on the internet to publicly expose and shame the person targeted.[2] It is often accompanied by other forms of harassment, such as the non-consensual sharing of intimate images. It is a gendered form of harassment, and women, especially from minority groups, are more likely to be subjected to doxing, which disproportionately impacts women of colour and LGTBQI+ communities.[3]

Researchers have suggested that there are three types of doxing: de-anonymising, or revealing someone's identity; revealing someone's personal and private information that allows them to be physically located; and releasing private information to undermine someone's credibility or reputation and to shame and humiliate them.[4]

Doxing can lead to the victim receiving large numbers of abusive messages and threatening phone calls, and in some cases, exposes them to physical violence. One example of this is when sexually explicit images or videos are posted on specialised advertising sites for prostitution together with private information, such as a woman's home address.

Digital violence, such as this, limits the participation of women in society and increases the digital gender divide.

Governments must apply feminist and intersectional thinking and use existing international human rights frameworks to draw up laws that protect women and other vulnerable groups from technology-facilitated gender-based violence like doxing.

WHERE DOES "DOXING" COME FROM?

Doxing, an abbreviation for "dropping documents" or 'dox,' is a malicious form of online abuse that consists of disclosing someone's personal information without their permission. Originating in the era of internet forums and chat rooms, doxing was initially about stripping away the anonymity of users in chatrooms and online forums who commonly hid their real identities behind pseudonyms. The rise of social media and online publishing, as well as the increased crossover between online and offline space, has made the practice of using one's true identity online the norm, with many internet users and assuming that keeping particular personal details private offers some level of protection against potential harms. In this context, doxing has become the practice of revealing real-world personally identifiable information about a target,such as their addresses, family members or workplaces, private information about relationships, behaviors and activities. This has been done with the intention of punishing, intimidating, or embarrassing affected individuals, or escalating online disputes into tangible threats.

WHAT IS INVOLVED IN A DOXING ATTACK?

Doxing attacks cover a spectrum of actions, from minor nuisances such as unsolicited sign-ups to services using the victim's name and address, to more grave risks like family or employer harassment, identity fraud, cyberbullying, and direct harassment and stalking. These personal details may be circulated within specific groups and communities to increase the scope of the attack (creating "the mob") or publicly disclosed on platforms like social media. Victims often remain oblivious to their information being public until they receive unexpected contact, such as phone calls to their personal or work numbers, highlighting the assumption of privacy being breached. Doxing is, however, not always evidence of a data breach. In some cases those carrying out a doxing attack might seek out publicly available information but still gather, distribute and publish it..

WHO DOES DOXING AFFECT AND HOW?

While doxing can target anyone when used as a cyberbullying or harassment tactic, those in the public eye are more commonly targeted by those who disagree with their opinions and beliefs. Like many other forms of online abuse, it disproportionately impacts women and girls, especially those with high profiles —journalists, politicians, and activists are particularly vulnerable.[5] The result of this form of abuse can be self-censorship, removal of online presence and profiles, or a reduction in online visibility and activity, in an attempt to restrict potential abuse.

2 European Institute for Gender Equality. 2023. Doxing. https://eige.europa.eu/publications-resources/thesaurus/terms/1460?language_content_entity=en

3 UNFPA, Technology-facilitated Gender-based Violence: Making All Spaces Safe (2021), p.15 https://www.unfpa.org/publications/technology-facilitated-gender-based-violence-making-all-spaces-safe

4 D. Douglas, "Doxing: a conceptual analysis", Ethics Information Technology, vol. 18, (2016), pp. 199–210.

5 https://www.icfj.org/sites/default/files/2023-02/ICFJ%20Unesco_TheChilling_OnlineViolence.pdf

KEY FINDINGS IN THE DIFFERENT JURISDICTIONS EXAMINED

INTERNATIONAL HUMAN RIGHTS LAW

Currently, there is no definition of "doxing" in any international human rights law, and international human rights law does not directly regulate or tackle "doxing." But there are provisions in some international human rights laws and standards that could be read as setting out member states' obligations to combat doxing:

The Universal Declaration of Human Rights states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[6] The malicious publication of an individual's private information could be seen as an arbitrary interference with their privacy. Whilst the respective State may not commit the violations, the State can use the provision to regulate platforms that enable such arbitrary publication of private information to protect its citizens.

The Council of Europe's Convention on Cybercrime (Budapest Convention), an international law regarding cybercrime, could apply in cases of doxing. For instance, Articles 2, 3 and 8 of the Convention provide that Member States should adopt legislative and other measures to criminally sanction illegal access and interception of data and computer-related fraud. As illegal access and interception of data are preparatory steps to doxing, this Convention can be considered part of the international legal framework to combat doxing.

EUROPEAN UNION

The term "doxing" is not defined under EU law. There is no specific EU regulation regarding doxing. Still, EU regulations on online illegal content and data protection, such as the General Data Protection Regulation (GDPR), may be relevant to prohibiting doxing.

A 2021 resolution from the European Parliament to the European Commission recognised doxing as a form of cyber violence that disproportionately affects women and girls. In March 2022, the European Commission adopted a proposal for a Directive on combating violence against women and domestic violence[7], which is relevant to doxing.

Article 8 of the proposed Directive makes it a criminal offence to make material containing the personal data of another person, without that person's consent, accessible to a multitude of end-users by means of information and communication technologies to incite those end-users to cause physical or significant psychological harm to the person.

Also, Article 9 makes it a criminal offence to initiate an attack with third parties directed at another person, by making threatening or insulting material accessible to a multitude of end-users, by means of information and communication technologies, with the effect of causing significant psychological harm to the attacked person.

The EU Digital Services Act (DSA)[8] could also be relevant to prohibiting doxing with respect to the removal of 'illegal content' by 'intermediary' services such as social media platforms. Doxing could be considered as 'illegal content' within the meaning of the DSA in Member States where it is expressly prohibited under national law.

For example, doxing is a criminal offence sanctioned by a fine of up to EUR 45,000 and three years of imprisonment in France. Article 223-1 of the French Criminal Code[9] prohibits the act of revealing, disseminating or transmitting information relating to the private, family or professional life of a person when such an act enables that person to be identified or located with the intention of exposing them or their family to a direct risk of harm.

In Germany, national civil law and fundamental rights are applicable, particularly when claiming an injunction. A court judgement in Hamburg[10] issued an interim injunction prohibiting the defendant from publishing the plaintiff's personal data without their consent.

Doxing could also qualify as a "personal data breach" under Article 4 of the GDPR.[11] The GDPR also provides victims the

6 Article 12 of the Universal Declaration of Human Rights
7 See further information in the Directive here: Ending Gender Based Violence
8 The Digital Services Act
9 French Criminal Code
10 Hamburg Regional Court (Judgement of 12.08.2021, Ref. 324 O 343/21)
11 https://gdpr-info.eu/art-4-gdpr/

right to correct inaccurate data (Article 16) and even have it erased (Article 17). However, the GDPR's applicability to "doxing" could be relatively limited because it only applies to processing personal data by automated means or to the non-automated processing of personal data that is, or is intended to be, stored in a filing system. It does not apply to personal data processed by a natural person during a purely personal or household activity.

AUSTRALIA

Currently, no statute or case law in Australia provides a legal definition of "doxing".

Currently, doxing is regulated under the Criminal Code Act[12], where it is an offence to use a carriage service (which includes the internet) to menace, harass or cause offence. The Criminal Code provides that the acts result in the offence when committed in a way that a reasonable person would regard them as being, in all circumstances, menacing, harassing or offensive. In considering whether the material is offensive, the Court shall take into account "the standards of morality, decency and propriety generally accepted by reasonable adults", "the literary, artistic or educational merit (if any) of the material", and "the general character of the material (including whether it is of a medical, legal or scientific character".For example, Australian courts have found sending threatening messages on Facebook[13] and sending unsolicited photos of genitals[14] as "offensive" under this Act. This offence carries a maximum of 3 years in prison.

In addition, a 2022 review of the 1988 Privacy Act by the Attorney General's Department of Australia[15] proposed regulating the use of other's personal information by individuals in their personal capacity. The proposal is still being considered, and if implemented, it would strengthen the protection of people against invasions of their privacy via doxing activities.

ENGLAND AND WALES

The term 'doxing' is not defined in English or Welsh law.

However, there are several avenues by which victims of doxing can seek compensation or criminal prosecution.

The Online Safety Act 2023[16] is a new law aiming to regulate the UK's online environment better. The Act contains content moderation provisions that put a greater responsibility on tech and social media platforms to remove certain material from their platforms under specific conditions. When the Bill was initially introduced, it contained adult safety duties that would criminalise 'legal but harmful' content on in-scope platforms. But these sections were removed in the final Act and replaced with transparency, accountability and freedom of expression duties. These provisions specify which types of legal content platforms would need to be addressed, under the duty to provide user empowerment. Some types of online platforms will also have to set clear terms of service in relation to the restriction or removal of user-generated content and may be required to remove content that goes against such terms. Under the Act, doxing may fall within the scope of the provisions mandating platforms to moderate and take down messages related to criminal offences. However, the scope of these provisions is limited as they relate only to the removal of doxing posts and do not necessarily criminalise the offence or mandate compensation for victims.

In addition to this, doxing may be unlawful under other criminal laws. For example, under the Protection from Harassment Act (PHA) 1997, there are two primary harassment offences under the PHA. There is an offence of harassment under Section 2 and harassment causing fear or violence under Section 4.

But for an incidence of doxing to amount to harassment, it would have to be part of a 'course of conduct' occurring over more than one occasion. Pursuing a conviction based on this offence is limited to occasions where there are multiple offending actions and may not be useful for a single doxing incident.

Doxing may also amount to a stalking offence under the same Act.[17] The Crown Prosecution Service Stalking and Harassment Guidance states that stalking may be understood as a pattern of Fixated, Obsessive, Unwanted and Repeated (FOUR) behaviour which is intrusive. Similar to the offence of harassment, stalking must be part of a course of conduct and must comprise more than one occasion of related actions.

If a doxing incident includes publishing any statement or other material relating or purporting to relate to a person or

12 Section 474.17 of the Criminal Code Act 1995
13 Agostino v Cleaves [2010] ACTSC 19
14 Grott v The Commissioner of Police [2015] QDC 142
15 https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988
16 https://www.legislation.gov.uk/ukpga/2023/50/enacted
17 Section 2A and section 4A of the Protection from the Protection from Harassment Act (PHA) 1997

monitoring the use of the internet, email, or another form of electronic communication by a person, it may amount to stalking. If the actions leading up to the offence occur in an online environment, this may amount to cyberstalking. Currently, there is no legal definition or legislation for cyberstalking, and the Crown Prosecution Service Stalking and Harassment Guidance[18] states that whether an action will be in the scope of the offence depends on the context of each case.

Doxing might also be described as sending an indecent or grossly offensive message and may be unlawful if it amounts to malicious communication under the Malicious Communications Act (MCA) 1988.[19]

A malicious communication is where someone sends a letter or any other form of communication of any description that is indecent, grossly offensive, threatening, or contains information which is false or believed to be false. The communication needs to be sent to another person with the intent to cause distress or anxiety. The Social Media Guidelines state that depending on the facts of the case, a message posted on social media may not amount to 'sending to another' as it needs to be addressed to a specific person.

Sending a communication with the intent to cause distress or anxiety may also amount to an offensive or threatening message under the Communications Act 2003.[20]

The scope is narrower than under the Malicious Communications Act as Section 127 of the Communications Act applies to communications only sent over a public communications network, but which are 'grossly offensive', 'indecent' or 'obscene'. It is not necessary to show that the message was addressed or received by someone, so it covers posting a message on a website.

Doxing may also be in the scope of a data protection claim for damages under the UK's data protection legislation. If the information used in a doxing incident amounted to 'personal data' under Article 4(2) UK GDPR[21], the victim may be able to bring a claim if they have suffered due to the violation of data protection laws.

If someone shares information relating to another person, and this amounts to personal data, then that person may have a claim that their personal data had been unlawfully processed. If, as a result of the doxing, the victim suffers physical or emotional distress, the quantum of damages could be much higher.

In the UK, you can claim damages for breach of privacy if your right to self-control over your private information was infringed. Article 8 of the European Convention on Human Rights[22] includes the 'respect for private and family life, his home and his correspondence'. UK courts have interpreted the right to privacy as a misuse of private information.

If someone shares personal information on a public platform, there is likely a reasonable expectation that they want it to remain private and be protected under Article 8 ECHR.
There are also some criminal offences related to the unlawful access of a computer or computer system to obtain information related to a doxing offence under the Computer Misuse Act 1990.[23]

SCOTLAND

There is no specific criminal offence of "doxing" in Scotland.

However, various principles and a patchwork of laws can be put together to make a case.

The first offence that could cover doxing is "Harassment". It is governed under section 8 of the Protection from Harassment Act 1997[24] and stipulates that every individual has a right to be free from harassment and, accordingly, a person must not pursue a course of conduct which amounts to harassment of another.

The second offence that could be committed when doxing is "Stalking". This is governed under section 39 of the Criminal Justice and Licensing (Scotland) Act 2010[25] and includes causing fear or alarm, including by publishing a statement or other material.

The third offence that could be committed when doxing is "Threatening or abusive behaviour". This is governed under section 38 of the Criminal Justice and Licensing (Scotland) Act 2010[26] and relates to causing fear or alarm.

18 https://www.cps.gov.uk/legal-guidance/stalking-or-harassment
19 https://www.legislation.gov.uk/ukpga/1988/27/section/2
20 https://www.legislation.gov.uk/ukpga/2003/21/section/127
21 https://www.legislation.gov.uk/eur/2016/679/article/4
22 https://www.echr.coe.int/documents/d/echr/guide_art_8_eng
23 https://www.legislation.gov.uk/ukpga/1990/18/section/1
24 https://www.legislation.gov.uk/ukpga/1997/40/section/8
25 https://www.legislation.gov.uk/asp/2010/13/section/39
26 https://www.legislation.gov.uk/asp/2010/13/section/38

Provisions of the Online Harms Act[27] also apply in Scotland.

Other offences that could be relevant to individual cases of doxing might include that of defamation. Generally, the Defamation and Malicious Publication (Scotland) Act 2021[28] governs the common law offence of defamation in Scotland.

Another possible offence could be the unauthorised use of computer materials. The relevant provisions concerning doxing are governed under Sections 1 and 2 of the Computer Misuse Act.[29]

And finally, under Sections 45 and 47 of the Data Protection Act 1998[30] an individual subject to doxing has the right to protect their freedom of privacy by accessing their data as a data subject that a controller is processing and the right to erasure or to restrict the processing of their data. The latter two rights are based on a balancing act against public interests and are not absolute rights.

KENYA

Kenya has no specific law defining "doxing". However, it does have laws that prohibit doxing.

Under the Kenyan Constitution, 2010[31], Article 31 provides for the right to privacy, which includes the right not to have information relating to one's family or private affairs unnecessarily required or revealed. Article 33(1) guarantees every person the right to freedom of expression. However, in exercising the right to freedom of expression, one must respect the rights and reputation of others. Therefore, it is without a doubt that doxing contravenes Article 31 and is likely to constitute an abuse of the right to freedom of expression in terms of Article 33.

In addition, the Computer Misuse and Cyber Crimes Act 2018[32] criminalises cyber harassment, identity theft or impersonation of any person. If a person wilfully communicates with another person or anyone known to that person, and if they know or ought to know that their conduct is likely to cause those persons apprehension or fear of violence to them or damage or loss on that person's property; or detrimentally affects that person; or is in whole or part, of an indecent or grossly offensive nature and affects the person, then they have committed an offence. The offence carries penalties of up to 20 million shillings or imprisonment of up to 10 years.

The Data Protection Act[33] also provides a regulatory framework for data protection and guidelines on collecting, using, storing or sharing personally identifiable data. It is likely that this piece of legislation, to a certain extent, regulates doxing in Kenya.

Regarding the development of future laws, The Personal Data Protection Guidelines for Africa 2018[34] and the National Information, Communications and Technology (ICT) Policy 2019[35] could provide a helpful basis for future law-making in this area.

NEW ZEALAND

Doxing is not defined under New Zealand law. However, the act of doxing is likely to fall within the broad definition of 'harmful digital communication' under the Harmful Digital Communications Act 2015 (HDCA)[36].

Harmful digital communication refers to communication that does not adhere to the HDCA's 'communication principles', which state that digital communication must not:

- disclose sensitive personal information;
- be threatening, intimidating, or menacing;
- be grossly offensive to a reasonable person in the position of the affected individual;
- be used to harass an individual;
- contain a matter that is published in breach of confidence;
- incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual;

In short, the HDCA made three key changes.

1. Establishing Netsafe as the approved agency to deal with cybercrimes (including doxing)
   While the agency has no authority to investigate or prosecute perpetrators, Netsafe is empowered to advise victims and to assist both parties in seeking a resolution through mediation.

27 https://www.legislation.gov.uk/ukpga/2023/50/enacted
28 https://www.legislation.gov.uk/asp/2021/10/contents
29 https://www.legislation.gov.uk/ukpga/1990/18/contents/scotland
30 https://www.legislation.gov.uk/ukpga/1998/29/contents
31 http://www.parliament.go.ke/sites/default/files/2023-03/The_Constitution_of_Kenya_2010.pdf
32 http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf
33 Data Protection Act 24 of 2019
34 https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/
35 https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf
36 https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html

2. Implementing criminal penalties
The significance of the HDCA is that it establishes a criminal regime for dealing with digital communications that cause serious emotional harm. The Police determine whether the threshold of emotional distress has been reached. Any person convicted of causing harm by posting a harmful digital communication can be imprisoned for up to 2 years or pay a fine of up to $50,000.
Several individuals have already been prosecuted under the HDCA. For instance, Margaret Herewini-Te Huna was sentenced for posting harmful digital communication after posting private information about her victim, such as where the victim lived and worked.[37]

3. Empowering the District Court to impose penalties on perpetrators and to issue take-down notices to host sites

The Act also offers a safe harbour and protection from civil and criminal liability for online content hosts who comply with the notice-takedown procedure established by Section 24.

In addition, New Zealand has developed a body of common law principles that protect against the invasion of an individual's privacy, which could be used in cases of doxing.

NIGERIA

The term "doxing" is not defined under any Nigerian legislation. There are, however, laws that prohibit the act of doxing.

Section 37 of the Nigerian Constitution[38] provides that "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected". The breach of the privacy of individuals may generally be viewed as - an intrusion of personal life (with regard to how that information was obtained), publicity given to private life, and wrongful appropriation. A victim of doxing may bring an action for breach of his or her constitutional right to privacy if they can successfully persuade the court to construe the constitutional right to privacy as a right covering the intrusion of one's private life.

The Violence Against Persons (Prohibition) Act 2015[39] (VAPP) was enacted to prohibit all forms of violence against persons in private and public life. The VAPP Act covers a wide range of offences offline that may also apply online. Provisions of the VAPP Act criminalise coercing another person to act to the detriment of an individual's physical or psychological wellbeing (causing emotional, verbal and psychological abuse on another), intimidation, indecent exposure and stalking. The act of doxing could be said to fall under the remit of this legislation.

The Nigerian Data Protection Act 2023[40] [41] contains provisions promoting data processing practices that safeguard personal data security and data subjects' privacy. The definition in the Act used for 'personal data' closely tracks Article 4(1) of the GDPR.
Regarding potential future laws, the Digital Rights and Freedom Bill 2019[42] contains provisions guaranteeing privacy, assembly, and association online. Specifically, one of the objectives of the proposed law is to "accord data privacy more priority in the digital age". Part III of the Bill proposes criminalising hate speech and other acts inciting hostility or discrimination. If passed into law, the provisions would provide legislative safeguards to victims.

SOUTH AFRICA

The term "doxing" in the Republic of South Africa does not have a legal definition.

The concept of doxing is not governed by one umbrella legislation. It depends on how the doxing takes place. So, various laws within South Africa can apply to doxing.

First is the Cybercrimes Act of 2020,[43] which provides for crimes committed online. This legislation will apply where private information is published on the internet (often the case with doxing). Sections 14 and 15 of the Cybercrimes Act also make it a criminal offence to send a data message inciting damage to property or violence or to threaten a person with such, which is frequently the end product of doxing.

Second is the Protection of Personal Information Act of 2013[44] (POPIA). Since doxing relates to the action or process of searching for and publishing private identifying information

37 https://districtcourts.govt.nz/assets/unsecure/2018-11-30/2018-NZDC-20574-Police-v-Herewini-Te-Huna.pdf
38 https://nigerian-constitution.com/chapter-4-section-37-right-to-private-and-family-life/
39 https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/104156/126946/F-1224509384/NGA104156.pdf
40 Future of Privacy Forum. 2023. Nigeria's New Data Protect Act Explained https://fpf.org/blog/nigerias-new-data-protection-act-explained/
41 https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf
42 https://placng.org/i/wp-content/uploads/2019/12/Lead-Debate-and-Provisions-of-the-National-Assembly-Digital-Rights-and-Freedom-Bill-2018.pdf
43 https://cybercrimesact.co.za/
44 https://popia.co.za/

about a person, POPIA may apply. It will apply to doxing if the publicised information constitutes personal information and is not in the public domain as provided under Section 9. This would result in an infringement on the right to privacy. POPIA defines 'personal information' broadly, but for our purposes, it may be defined as the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person and additional information such as an email address, a physical address, a telephone number, location information, online identifier, or other particular assignment to the person.

Third is the Protection from Harassment Act of 2011[45], which could be triggered when doxing involves harassing behaviour.

Lastly, the Domestic Violence Amendment Act[46] has extended the definition of intimidation to include communication by electronic means, and this is often the nature of doxing.

USA

There is no formal definition of "doxing" in federal law. However, some laws exist at the state level.

California

The general concept of doxing is addressed in the California Penal Code Section 653.2[47]. Under the Code, it is illegal to electronically distribute identifying information and/or digital images of a harassing nature to cause unwanted physical contact, injury, or harassment by a third party. A conviction under this law is a misdemeanour with a maximum prison sentence of one year. The statute also allows the assessment of a fine of up to $1,000.

A similar law, California Government Code Section 6218.01[48], applies to the personal information of healthcare-related personnel such as abortion clinic staff. The law makes it a crime to post personal information or an image of a provider, employee, volunteer, or patient and would increase the penalty to either imprisonment for one year, a fine of up to $10,000, or both that fine and imprisonment, and would increase the penalty for a violation resulting in bodily injury to $50,000.

Further guidance on statutory electronic harassment under the Penal Code is offered by People v. Shivers (2015)[49]. This case clarifies that the offence requires that "a reasonable person" must consider the electronic message likely to incite or produce unwanted physical contact, injury or harassment by a third party", which means the defendant's communication must "be likely to incite or produce that unlawful reaction." The "unlawful reaction" means "unwanted physical contact, injury or harassment."

California Penal Code Section 422[50] also covers intimidation caused by statements issued by an electronic device. And California Penal Code Section 646.9[51] covers harassment and stalking.

California Penal Code Section 422.55[52] also defines a hate crime as including a criminal act committed because of a victim's actual or perceived gender, which could be relevant if doxing is used as a means of violence towards women.

Texas

A new offence related to 'The Unlawful Disclosure of Residence Address or Telephone Number', Section 42.07452 of the Texas Penal Code, which covers doxing, has been brought in for Texas. It came into effect on September 1, 2023.

This new offence was designed to target internet posts that disclose a person's residence address or telephone number with the intent to cause harm or a threat of harm to the individual or a member of the individual's family or household.

A person commits an offence if the person posts the residence address or telephone number of an individual on a publicly accessible website with the intent to cause harm or a threat of harm to the individual or a member of the individual's family or household.
Depending on the circumstances, the crime is punished as a Class B or a Class A misdemeanour. The offence is a Class

45 Protection from Harassment Act 2011
46 https://www.gov.za/documents/domestic-violence-amendment-act-14-2021-28-jan-2022-0000
47 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=653.2
48 California Government Code
49 https://casetext.com/case/people-v-shivers-34
50 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=422.&lawCode=PEN
51 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=646.9&lawCode=PEN
52 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=422.55.&lawCode=PEN

A misdemeanour if it results in the bodily injury of the doxing victim or any member of the doxing victim's family or household; otherwise, it is a Class B misdemeanour.

Not all commonly understood practices of doxing are currently illegal under this new law. For instance, it does not include releasing personal photos of an individual, releasing information about an individual's family, work or other private information, and encouraging others to use released information to harass an individual.
However, other laws may apply to those situations, such as laws in the Penal Code on Harassment and Stalking.[53]

Virginia

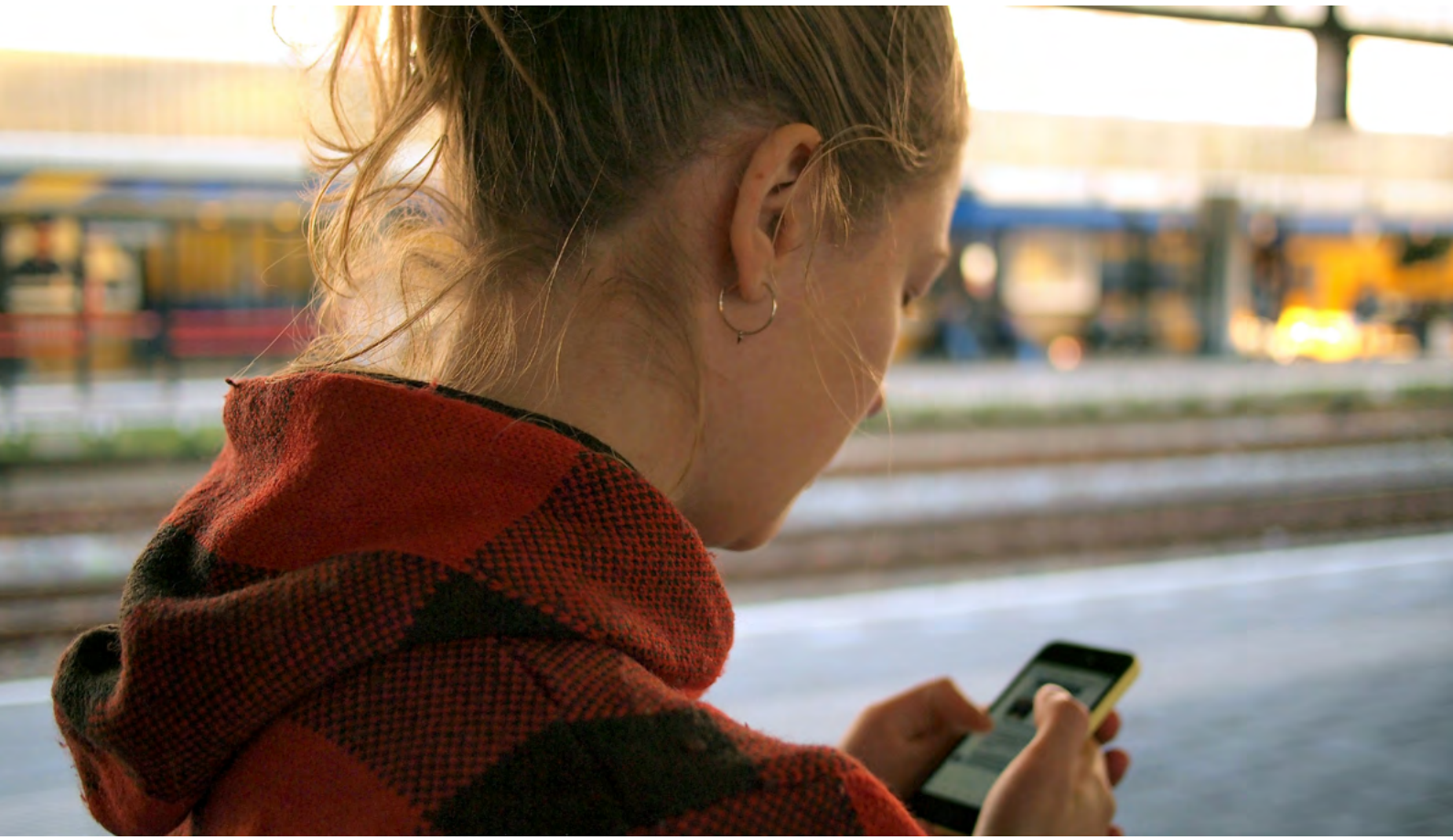
While there are no laws specifically prohibiting doxing, harassment by computer, threats, and stalking are all unlawful under Virginia law.

Virginia prohibits the use of a computer to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act with the intent to coerce, intimidate or harass.[54]

The Code of Virginia also prohibits publishing of a person's name or photograph or identification of the person's primary residence address with the intent to coerce, intimidate or harass.[55]

More severe forms of doxing may implicate Virginia's prohibition against using a computer to stalk another person. Doxing may also be found to be a bias-based crime in relation to Virginia's hate crime law.

53 https://statutes.capitol.texas.gov/Docs/PE/htm/PE.42.htm#42.074
54 Virginia Code Ann. § 18.2-152.7:1
55 Virginia Code Ann. § 18.2-152.7:1



RECOMMENDATIONS

The absence of comprehensive laws addressing doxing poses a significant challenge in our increasingly digitised society. Doxing, the malicious act of publicly disclosing private and sensitive information about individuals without their consent, has become a potent tool for harassment, intimidation, and the infringement of personal privacy. The lack of specific legislation to combat and penalise such actions leaves victims vulnerable and without adequate legal recourse.

- Governments need to review existing laws and see if they apply to doxing and take into account the gendered nature of this form of online abuse. This means ensuring that the laws, which should be aligned to international human rights law and standards, are adaptable to evolving technologies, that they provide for the offline impacts of online behaviours, that they are easy for victims to use to seek redress, and that they provide meaningful consequences for perpetrators. If no existing laws apply, new laws must be enacted.

- Governments and the tech industry also need to cooperate and implement effective mechanisms to address technology-facilitated gender-based violence nationally and across borders. This includes adapting existing mechanisms for multilateral international cooperation and ensuring that victims can access criminal justice and other remedies wherever they live.

- There must also be laws and standards that hold tech platforms accountable for cooperating with law enforcement agencies within and across borders and ensuring that they proactively identify harms and perpetrators and take swift actions to respond to incidents.

BRIEFING PAPER: DOXING, DIGITAL ABUSE AND THE LAW

CONTACT EQUALITY NOW

info@equalitynow.org

www.equalitynow.org

@equalitynoworg

@equalitynow

@equalitynoworg

CONTACT AUDRi

www.audri.org

@AUDRi

@AUDRights

Equality Now
A just world for women and girls.

Alliance For Universal Digital Rights