# Regulating Image-Based Abuse: An Examination of Australia's Reporting and Removal Scheme

Melanie Burton, Savannah Minihan, Mariesa Nicholas, Jason Connor, and Kylie Trengove

**Abstract.** Image-based abuse (IBA) is a form of technology-facilitated abuse that involves the creation, sharing, or threatened sharing of intimate images without the consent of the person pictured. In Australia, the eSafety Commissioner (eSafety) oversees the IBA reporting and removal scheme (IBA scheme), with regulatory powers set out under the Online Safety Act 2021. eSafety is the first government agency to implement a dedicated scheme responsible for facilitating the removal of non-consensual intimate images posted online via the establishment of an IBA reporting portal and a civil penalties scheme. This research was conducted by eSafety staff who examined the operation of eSafety's IBA scheme from 2018 to 2023. Under the operation of the IBA scheme, eSafety has been handling a growing volume of reports, which have increased by more than 960%, from 849 reports in 2018/19 to 9,060 reports in 2022/23. This has been led by an unanticipated increase in reports of sexual extortion, from 432 in 2018/19 to 6,187 in 2022/23. This paper examines what was being reported under the scheme, including who was reporting and changes in report numbers over time.

## 1 Introduction

In recent years, image-based abuse (IBA) has become an increasingly pervasive social and legal problem (Henry and Witt 2021; Yar and Drew 2019). In response, a consensus among policymakers, law enforcement, and researchers has emerged that action needs to be taken to prevent and respond to IBA, including through the development of new regulatory schemes.

Australia has been at the forefront of IBA regulation. In seeking to overcome barriers to reporting often faced by victims of IBA, in late 2017 the Australian government funded the eSafety Commissioner (hereafter referred to as eSafety), Australia's independent



doi:10.54501/jots.v2i5.222

regulator for online safety, to establish a service to assist IBA victims[1] to report their experiences and to seek removal of IBA material. eSafety became the first statutory government body to provide a support-oriented response for victims of IBA that did not require engagement with law enforcement or the criminal law system. eSafety operates a portal where reports can be made, and where advice and resources focused on understanding, responding to, and managing the impact of IBA can be found (eSafety Commissioner 2017b). As other countries set out to develop their own responses to IBA, much can be learned from the experiences of eSafety's IBA reporting and removal scheme (IBA scheme).

This study contributes to the evidence base by examining how the IBA scheme has operated over its first five years. This paper provides insights from practice into the role that governments in other countries can play in IBA regulation, by providing a descriptive examination of eSafety's experience in receiving reports under the IBA scheme. This paper will draw from eSafety's quantitative reporting data from August 18, 2018, to June 30, 2023, to detail features of the IBA scheme, including what is covered by the current scheme. Specifically, the paper will address the following research questions:

- **RQ1:** How many reports, and from whom, did eSafety's IBA scheme receive between 2018 and 2023?
- **RQ2:** What were the most common categories of IBA behavior reported to the scheme?
- **RQ3:** How did the prevalence and nature of reports to the IBA scheme change over time?
- **RQ4:** Which platforms and services were most frequently associated with reports to the IBA scheme?
- **RQ4:** What actions did eSafety take in response to reports of IBA?

Our examination found that eSafety's IBA scheme has increasingly facilitated the removal of harmful content and enabled Australian victims of IBA to access expert assistance, regain control over their situation, and receive practical support to help them feel safer online. In particular, our findings revealed that, under the operation of the IBA scheme, eSafety has been handling an increasing volume of reports, growing by more than 960%, from 849 reports in 2018/19 to 9,060 reports in 2022/23. This has been led by an unanticipated increase in reports of sexual extortion, from 432 in 2018/19 to 6,187 in 2022/23, with young males being the most common victims reporting sexual extortion to the scheme. We additionally found that Instagram and Snapchat were the most common platforms mentioned in complainants' reports to the scheme. In addition to providing

1. This paper acknowledges that people who have experienced image-based abuse will identify with different terms relating to their experience. The importance of individual choice is recognized. While this paper uses the terms "victim(s)" and "complainant(s)" to refer to those who experience and/or report IBA, the use of other descriptors, such as "victim-survivor(s)," are also recognized and supported.

complainants with education, referrals, information, and advice, the IBA scheme enables eSafety to engage with platforms directly to facilitate the removal of material. We found that eSafety generally had high success rates when engaging with platforms, including when reporting user behavior (i.e., perpetrator accounts) and requesting the removal of non-consensual images.

## 2 Image-Based Abuse

Advances in digital technology (e.g., camera and internet-enabled devices, streaming services, artificial intelligence, cloud computing, and peer-to-peer networking) (Henry and Flynn 2019) have provided the opportunity for new ways for sexual violence to be perpetrated (McGlynn and Rackley 2017), including technology-facilitated sexual violence (Henry, Flynn, and Powell 2018). One category of technology-facilitated sexual violence is image-based abuse (IBA), which includes three key forms: non-consensual creation or possession of intimate images; non-consensual distribution of intimate images; and threats to share intimate images (Henry and Flynn 2019; Henry et al. 2020; Powell and Henry 2017; Powell, Henry, and Flynn 2018; Powell et al. 2019).

IBA first surfaced in the public consciousness in the early 2000s, associated with vengeful acts of humiliation that were largely perpetrated by former romantic partners, under the media-derived rubric of "revenge porn" (Yar and Drew 2019). The more recent shift to incorporate and adopt broader terminology—including "image-based abuse" (eSafety Commissioner 2017a), "image-based sexual abuse" (McGlynn et al. 2021), "non-consensual intimate image abuse" or "non-consensual dissemination of intimate images" (Semenzin and Bainotti 2020; StopNCII.org, n.d.), and "non-consensual pornography" (Falduti and Tessaris 2023; Ryan 2018)—indicates an understanding that the problem is complex and diverse, moving away from victim-blaming connotations and the vengeful ex-partner narrative (Maddocks 2018; Rigotti, McGlynn, and Benning 2024). IBA includes the sharing, or threatened sharing, of intimate images without consent that may have been created by the victim as a "selfie" and/or produced consensually in the context of an intimate relationship, but also includes images created coercively or taken during a sexual assault, covertly produced images (e.g., "downblousing," "upskirting," or surreptitious filming) (Henry, Flynn, and Powell 2019), digitally altered imagery where a person's face or body is superimposed onto a pornographic photo or stitched into a video (e.g., "deepfakes" and digitally altered imagery abuse) (Flynn et al. 2021), and images that have been hacked or stolen before being shared online (Flynn and Henry 2019; Stokes 2015). When these types of images are shared and/or created without the consent of the victim, it is IBA. IBA also includes sexual extortion (also known as sextortion or webcam blackmail). This occurs when someone threatens to share an intimate image unless the victim gives into their demands (usually for money, in the case of financial sexual extortion, but it can also be for more intimate images or sexual favors) (eSafety Commissioner, n.d.). In addition, the creation, sharing, or threatened sharing of intimate

images of children, in most instances, constitutes child sexual exploitation material (CSEM) (Australian Centre to Counter Child Exploitation 2021).

Perpetrators of IBA are not only current or former partners, but may also include family members, friends, acquaintances, and persons unknown to the victim, including organized criminal groups (Eaton, Ramjee, and Saunders 2022; Finkelhor et al. 2023; Henry, Flynn, and Powell 2019; Henry and Umbach 2024; Papachristou 2023; Patchin and Hinduja 2024; Powell et al. 2022; Thorn and National Center for Missing and Exploited Children 2024). In addition, the motivations behind IBA extend beyond revenge to include control (e.g., in the context of domestic and family violence) (Dragiewicz et al. 2018; Harris and Woodlock 2019), sexual gratification, monetary gratification (e.g., in the context of financial sexual extortion), harassment, humiliation, misogyny and entitlement, and bullying or status-seeking among peers (e.g., when nude images circulate without consent among peers in a school context) (Bindesbøl Holm Johansen, Pedersen, and Tjørnhøj-Thomsen 2018; Eaton et al. 2020; eSafety Commissioner 2017a; Henry, Flynn, and Powell 2019; Scott et al. 2022). IBA also frequently co-occurs with other forms of abuse, such as unwanted communications, threats of harm, controlling behavior, or physical harm (Powell et al. 2022).

In a global systematic review and meta-analysis of technology-facilitated abuse (n = 19 papers), pooled prevalence of victimization rates found that 8.8% of participants across 20 independent samples had their intimate images shared without consent, 7.2% had been threatened with distribution of intimate images, and 17.6% had experienced non-consensual creation of sexually explicit material (Patel and Roesch 2022). A survey conducted in 2016 in Australia found that one in five respondents had experienced IBA (Henry, Powell, and Flynn 2017). A more recent survey, conducted in 2019, involving 16- to 64-year old participants in Australia, New Zealand, and the United Kingdom (n = 6,109), reported that just over one in three respondents had experienced IBA (37.7%), with findings comparable across the three countries (Australia 35.2%, New Zealand 39.0%, and the United Kingdom 39.0%) (Powell et al. 2022). These findings suggest that the prevalence of IBA is increasing. Indeed, analysis of reports to the United Kingdom's Revenge Porn Helpline found a 106% increase in reports of IBA from 2022 to 2023, with reports involving sexual extortion largely accounting for the increase (Papachristou 2023). In regard to prevalence estimates of sexual extortion specifically, a recent large-scale survey of 16,693 adults from 10 countries found that, overall, 14.5% of respondents had received threats to share their intimate images (Henry and Umbach 2024). Looking at Australian respondents only, the prevalence was 15.9% (Henry and Umbach 2024).

Some studies have found gendered differences in IBA prevalence rates, with studies to date largely exploring gendered dynamics between women and men. Some studies have found that women experience non-consensual sharing of intimate images at higher rates than men (eSafety Commissioner 2017a; Papachristou 2023), and others report higher

prevalence rates among men (Powell and Henry 2017; Powell et al. 2022; Reed, Tolman, and Ward 2016). Other studies, conversely, indicate that men and women experience non-consensual sharing of intimate images at similar rates (Lenhart, Ybarra, and Price-Feeney 2016; Gámez-Guadix et al. 2015). However, there are gendered patterns in the nature, extent, and impacts of the victimization (Henry, Flynn, and Powell 2019; Powell et al. 2020). For example, recent large-scale surveys and reporting data have generally shown that boys and men are more likely than girls and women to receive threats to share intimate images, especially in the context of financial sexual extortion (Eaton, Ramjee, and Saunders 2022; Henry, Flynn, and Powell 2019; Henry and Umbach 2024; Papachristou 2023; Powell et al. 2022; Thorn and National Center for Missing and Exploited Children 2024). A recent report that analyzed complaints to the United Kingdom's Revenge Porn Helpline during 2023 found that 93% of reports involving sexual extortion affected men, whereas over 70% of reports involving threats to share or intimate images being shared without consent (which didn't involve sexual extortion) affected women (Papachristou 2023). Women were also disproportionately impacted by the quantity of intimate images shared without consent: women had approximately 28 times more images shared without their consent, compared with men (Papachristou 2023). Analysis of reports to the National Center for Missing and Exploited Children (NCMEC) CyberTipline from 2020 to 2023 similarly showed that 90% of victims of financial sexual extortion were males aged 14–17, whereas sexual extortion that involved demands for content, or other demands such as returning to or entering into a romantic relationship, most commonly involved female victims (Thorn and National Center for Missing and Exploited Children 2024). The types of IBA that boys/men and girls/women are more at risk of, therefore, seemingly differ. However, further research is needed to explore nonbinary and gender-diverse individuals' experiences of IBA.

Regarding age differences, research indicates that younger adults experience IBA at greater rates compared with older adults (Eaton, Ramjee, and Saunders 2022; Henry and Umbach 2024; Powell et al. 2022). For example, in the aforementioned survey examining the prevalence of threatened image sharing across 10 countries, adults aged 18–24 were the most frequent victims, with 22.9% of 18–24-year-old respondents having received threats to share their intimate images (Henry and Umbach 2024). Additionally, while large-scale surveys would suggest that the prevalence of IBA is higher among adults compared with young people (those under 18 years old), young people are nonetheless still at risk of experiencing IBA. IBA involving intimate images of children, in most instances, constitutes child sexual exploitation. A recent survey of 1,953 adolescents residing in Australia found that 11.3% had experienced sexual extortion in their lifetime (Wolbers et al. 2025). In addition, a nationally representative survey of 4,972 teenagers aged 12–17 in the United States conducted in 2019 found that approximately 5% of respondents had experienced sexual extortion (Patchin and Hinduja 2024). As with survey findings among adults, these findings suggest that the prevalence of IBA among young people is also increasing. Indeed, mirroring reporting data among adults (Papachristou 2023), analysis of NCMEC CyberTipline data similarly showed an increase in reports of sexual

extortion from 2020 to 2023, an increase largely driven by reports involving financial sexual extortion (Thorn and National Center for Missing and Exploited Children 2024). Furthermore, the Internet Watch Foundation observed a 19% increase in reports of child sexual abuse related to sexual extortion in the first six months of 2024, compared with the same period in 2023 (Internet Watch Foundation 2024). While the majority of victims were aged 16–17, there was a 25% increase in reports involving 14–15-year-olds, with some victims as young as 11, indicating that victims of sexual extortion are getting younger (Internet Watch Foundation 2024).

With the rapid and evolving development of social media, online dating, and other networked technologies, and increased online social engagement (i.e., in the context of the global COVID-19 pandemic), the prevalence of all forms of IBA is not only increasing (Henry et al. 2020), but is also having significant psychological, physical, and social impacts on those involved (eSafety Commissioner 2017a; Henry, Flynn, and Powell 2019; Liggett O'Malley and Smith 2024; McGlynn et al. 2021; Patel and Roesch 2022; Powell et al. 2022; Schmidt et al. 2024). The risk of IBA is compounded by the growth and development of generative artificial intelligence: the increasing ease with which synthetic sexual content, such as deepfakes, can be created exacerbates the potential for IBA (Papachristou 2023; Umbach et al. 2024). As a result, growing global attention has been paid to the problem of IBA over the last decade (Henry, Flynn, and Powell 2018, 2019).

### 2.1 Responding to image-based abuse

Initial responses to IBA were centered on victims seeking out content and requesting removal by designated internet services, relevant electronic services, and social media services (Yar and Drew 2019). However, more recently, there has been a shift from voluntary to statutory regulation, and from civil to criminal responses evidenced through the introduction of new criminal laws and offenses, civil law reviews and reforms, and high-level policy initiatives across the world (e.g., in Australia, Belgium, Canada, the European Union, France, Germany, Italy, New Zealand, Spain, and the United Kingdom) (Falduti and Tessaris 2023; Flynn and Henry 2019; Franks 2017; Haynes 2021; McGlynn and Rackley 2017; McGlynn et al. 2021; Rigotti, McGlynn, and Benning 2024). Governments are also taking legislative steps to combat the creation and distribution of synthetic sexual content. For example, the Australian government recently passed the Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 (Cth) (Parliament of Australia 2024), which will impose criminal penalties on those who non-consensually share sexually explicit material, including non-consensual deepfake sexually explicit material. The United Kingdom government similarly progressed the Criminal Justice Bill through Parliament, which includes offenses around the creation of synthetic sexual content, as well as around the non-consensual taking or recording of intimate images (Papachristou 2023). This shift in responses to IBA has been supported by the implementation of new crime prevention and control schemes that focus on empowering victims and encouraging

reporting that leads to prosecution (Yar and Drew 2019).

Encouraging and facilitating IBA reporting is important for at least three key reasons. First, it can enable responsible regulatory agencies and law enforcement to respond to victim reports of IBA. This can give victims a degree of control back, can lead to the perpetrator being held accountable and may, in turn, reduce recidivism and perpetration. Second, reporting is necessary to understand the prevalence of IBA, including the characteristics of victims and perpetrators and IBA's social and emotional impacts on those involved. Third, reporting data enables regulatory and law enforcement agencies to understand offender methodology and to gather intelligence about modus operandi—information that can be shared between agencies to facilitate prevention and remediation efforts. Such information also facilitates identification of indicators or features on social media services that are relevant to the perpetration of IBA. Without accurate data on the prevalence and nature of IBA, it is difficult to design and determine the impact of interventions to reduce its occurrence (Yar and Drew 2019). However, encouraging victims to report experiences of online harm, including IBA, is a challenge due to concerns and fears about reporting, and a lack of knowledge about how and where to report their experiences (van de Weijer, Leukfeldt, and Bernasco 2018; Yar and Drew 2019). Victims of IBA may avoid reporting to law enforcement out of fear that they will feel shame or that they will experience victim-blaming (Dodge 2023; Flynn and Henry 2019; Rackley et al. 2021).

The criminalization of IBA is important to punish perpetrators and provide justice to victims. However, criminal offenses and civil schemes are limited in their capacity to prevent IBA or minimize its harm once images are posted online (Henry and Witt 2021). This is due to the ease with which images can be created, shared, uploaded, and downloaded; the speed with which images can disappear after being downloaded; and the copying and republishing of images across platforms and devices, making it difficult to prevent further distribution (Flynn and Henry 2019). Further, perpetrators of IBA are often difficult to identify due to the availability of anonymity measures (e.g., proxy servers and virtual private networks) (Henry and Witt 2021), and law enforcement can be limited in their capacity to investigate reported cases of IBA due to cross-jurisdictional and trans-geographical boundaries when perpetrators are located overseas (e.g., in sexual extortion cases) (Yar and Drew 2019).

Traditionally, many victims of IBA have not engaged with formal legal options (e.g., criminal actions), as the victims often prioritize the rapid removal of images (Rackley et al. 2021) over seeking action against the perpetrator. Further, some victims who know the perpetrator may not be willing to report their peers, family members, friends, partners, or ex-partners, as they do not want to criminalize those in their lives (Dodge 2023; Rackley et al. 2021). Until recently, legal options have not provided opportunities to prevent IBA or the support needed to minimize the its harmful impacts (Dodge 2023). Additionally, the prolonged timelines of some legal pathways are not appealing to IBA victims whose central concern is rapid image removal (Stevenson-McCabe and Chisala-Tempelhoff

2021).

Internationally, there has been growing recognition of the lack of transparency from platforms around how they moderate content, as well as the power platforms have over what users can share and encounter online and the discretion they have to create and enforce their own rules and guidelines (Henry and Witt 2021). In light of this and in response to the complex challenges of responding to IBA, governments are focusing on the introduction of new regulatory schemes to attempt to better hold technology companies accountable for hosting harmful content, including IBA, on their servers (Henry and Witt 2021).

## 3 The Evolution of the Australian eSafety Commissioner and the Image-Based Abuse Scheme

eSafety was first established in 2015 as the Children's eSafety Commissioner by the Enhancing Online Safety for Children Act 2015 (Cth) (Parliament of Australia 2015b), which saw the establishment of the world's first complaints scheme to tackle youth-based cyberbullying. In 2017, the legislation was renamed the Enhancing Online Safety Act 2015 (Cth) (Parliament of Australia 2015a) and eSafety's remit was expanded to include powers relating to illegal and restricted online content under Schedules 5 and 7 of the Broadcasting Services Act 1992 (Cth) (Parliament of Australia 1992).

In 2018, the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018 (Cth) (Parliament of Australia 2018) was passed. This expanded eSafety's remit to include powers relating to the non-consensual sharing of intimate images and established many of eSafety's current powers relating to IBA. In January 2022, the Online Safety Act 2021 (Cth) (the Act) (Parliament of Australia 2021a) took effect. eSafety's powers relating to IBA that existed under the Enhancing Online Safety Act 2015 were transferred to the Online Safety Act.

### 3.1 The Online Safety Act and eSafety's image-based abuse scheme

The Online Safety Act provides for eSafety's IBA scheme, conferring powers on eSafety when an intimate image has been shared without the consent of the person depicted in the image or when there has been a threat to share an intimate image without the person's consent. Importantly, eSafety does not have specified powers to deal with the creation of an intimate image.[2]

The Act provides that an intimate image must meet two requirements. First, it is a still or moving visual image that depicts, or appears to depict, any of the following: a person's

2. While eSafety does not have specified powers to deal with the *creation* of an intimate image, it does have the power to deal with the *possession* of material that contravenes the Section 75 prohibition (i.e., the person has shared or threatened to share an intimate image of a person without their consent) via remedial direction.

genital area or anal area, whether bare or covered by underwear; a person's breast(s) if the person identifies as female, transgender, or intersex; a private activity (e.g., in a state of undress, using the toilet, showering, having a bath, engaged in a sexual act of a kind not ordinarily done in public); or a person without attire of religious or cultural significance if they would normally wear such attire in public. Second, the image or video must also show the person in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy (i.e., in circumstances where the person would have assumed they had privacy). Notably, the definition of "intimate image" includes images that "appear to depict" a person. This includes "deepfakes" and images that are doctored or edited to look as though they depict a specific person, even if that is not actually the person in the image (Parliament of Australia 2021a).

The second requirement narrows the circumstances in which an image that contains or depicts certain content can be considered an "intimate" image and involves consideration of circumstances around the image's creation. For example, an image that depicts a person in a state of undress (such as an underwear model) and which is created and used for the purposes of a public advertising campaign is unlikely to meet the second requirement.

### 3.2 A closer look at the Act

There are four key provisions in the Act that relate to IBA. The first provision establishes a strong statutory prohibition against the non-consensual sharing of intimate images. Under Section 75 of the Act, a person must not share or threaten to share an intimate image depicting a person without that person's consent (Parliament of Australia 2021a). For Section 75 to apply, either the person depicted in the image or the person sharing or threatening to share the image must be ordinarily resident in Australia. While the Act does not create a criminal offense in relation to such conduct, if a person contravenes this Section, a civil penalty can be awarded.

Second, under the Act, eSafety has the power to accept complaints and objections about the non-consensual sharing of intimate images. A person can make a complaint to eSafety if they have reason to believe that someone has shared, or has threatened to share, an intimate image of them. A person may also make a complaint on behalf of another person if certain requirements are met; for example, if the victim is under 16, their parent or guardian can make a complaint on their behalf (Parliament of Australia 2021a).

eSafety can accept an "objection notice" from a person depicted in an intimate image (or on that person's behalf) when: an intimate image of the person has been provided on a relevant online service;[3] the intimate image is not an exempt image for the purposes of the Act (defined in Section 86 (Parliament of Australia 2021a)); and the depicted person is ordinarily resident in Australia, the end-user that posted the intimate image is ordinarily resident in Australia *or* the intimate image is hosted in Australia by a hosting

3. Defined in Sections 13, 13a, and 14, respectively, of the Act.

service.[4]

There are several key differences between an objection notice and a complaint. While a complaint can relate to the threat to share an intimate image, an objection notice must relate to the actual sharing of an intimate image. An objection notice can also be made by a person who previously gave consent, while a complaint must relate only to a person who has never given consent for the posting of the image.

The third key provision is eSafety's power to compel the removal of an intimate image by issuing a removal notice to the service provider or the end user (i.e., perpetrator). A removal notice requires the provider, or the end user, to take all reasonable steps to remove, or cease hosting, an intimate image. A person can be required to remove the material within 24 hours of being issued the notice. Removal notices are enforceable through injunctions and enforceable undertakings. Failure to comply may also be subject to formal warnings, an infringement notice, or civil penalty proceedings.

The fourth key provision enables eSafety to issue a remedial direction against a person that has shared or threatened to share an intimate image of a person without consent. A remedial direction requires the recipient to take specified action toward ensuring that they do not contravene Section 75 *in the future* (Parliament of Australia 2021a). The Act does not prescribe the specified actions that can be required, but they may include deleting material from a device and providing confirmation to eSafety.

Remedial directions are enforceable through injunctions and enforceable undertakings. Failure to comply may also be subject to formal warnings, an infringement notice, or civil penalty proceedings for up to 500 penalty units (Parliament of Australia 2021a).

## 4 Methods

This study uses de-identified reporting data collected from the IBA scheme from August 18, 2018, to June 30, 2023. Complainants can submit a report to the IBA scheme by completing an online form. Complainants indicate via the online form whether they need help with an intimate image or video that has been posted and/or help with threats to post an intimate image or video; whether the victim and/or perpetrator lives in Australia; whether the intimate image or video is of themself or another person whom they are entitled to make a complaint on behalf of; whether the victim was under 18 years old when the image or video was taken; the age and gender of the victim; and whether the intimate image or video shows the victim without religious or cultural attire they would normally wear when in public. Complainants also indicate whether the victim consented to the intimate image or video being posted;[5] they know the person who is responsible for posting or threatening to post the intimate image or video; they want the intimate

4. Defined in Section 17 of the Act.
5. This question only appears on the complaint form if the victim is aged 18 years old or older.

image or video removed; they want action taken against the perpetrator; they have any screenshots of or other information relevant to the complaint; the police are currently involved; and there is or has been a court order. Finally, the complaint form includes a number of free-text fields, where complainants are asked to provide further details about what happened, including where the content is located. Submission of the complaint form automatically generates a complaint on the system, which is then triaged and actioned by investigators from the eSafety IBA team, and, based on the details in the complaint form and any further information provided by complainants, categorized as a particular type of behavior.

The dataset was subjected to descriptive analysis using SPSS V29.0.2.0.

Special consideration was paid to the use of reporting data in the study. The Act confers functions relating to research on eSafety (Parliament of Australia 2021a), and the Australian Communications and Media Authority is required to provide eSafety with staff to assist the eSafety Commissioner to fulfill her functions and powers, under Section 184 of the Act. At the time this study was conducted, Australian privacy laws specifies that de-identified information ceases to be personal information once it has been de-identified. The use of de-identified information for these research purposes is therefore not restricted by the requirements that apply to use of personal information in the Privacy Act 1988 (Parliament of Australia 1988).

Strong protections were implemented to minimize the risk of re-identification, including de-identifying the data before it was provided for use in this research. The de-identified dataset was stored securely and only accessible by those conducting the research on a secure network drive. Further, to protect the identity of individuals reporting to eSafety, a number of free-text fields, such as those describing the report incidents in detail, were not included in the analysis. One free-text field provided details on where intimate images were located, but this field was de-identified prior to analysis. Because of this prior data de-identification, we are unable to determine the extent to which multiple complaints were made by one victim. It is possible that certain individuals were repeatedly targeted and filed multiple complaints to the scheme.

There were several other limitations to the interpretation of the data. First, each report to the IBA scheme is categorized by eSafety as only one type of behavior. However, the assigned category may not capture the entirety of a victim's experience. For example, a report categorized as sexual extortion may also involve images of an individual without their religious or cultural attire, digitally altered images, or recording without consent. Therefore, some categories of behavior are likely to be underrepresented in the reporting data, and the reporting categories presented here should not be considered to capture the entirety of a victim's experience. Additionally, these reporting categories have evolved over time, and consequently there is likely inconsistency in how categories have been used throughout the duration of the reporting period.

Second, while this research sheds light on the content and behaviors reported to and managed by eSafety under the IBA scheme, we cannot infer that this constitutes or represents all patterns of IBA experienced. Not all victims of IBA are able or willing to report and/or seek help for their experience(s). Further, while this research indicates patterns in the reporting and managing of reports under the IBA scheme, it can only provide an indication of the *types* of IBA experienced in the Australian population; it is not indicative of the *prevalence* of IBA in Australia. Additionally, this paper lacks the lived experiences, perspectives, and insights of those who have accessed the scheme. While the rates at which eSafety was successful in having IBA content removed from platforms provides an indication of the success of the scheme, future research could complement data from reporting schemes with complainants' feedback and reflections after accessing the scheme.

A third limitation is that the dataset reflects the status and categorization of reports from when data were extracted. For reports where there was subsequent or ongoing investigation and evolving factors or outcomes, the data may have changed after the creation of the database (e.g., report categories and actions taken by eSafety). Thus, the data should be interpreted with this in mind.

The fourth limitation to the interpretation of the data is inconsistency in terms used and platform names provided by complainants in the free-text field for location of content. Due to the sheer volume of reports, this data was first coded in an automated manner using SPSS syntax by searching the free-text field for key location terms, including common misspellings. For example, any responses that contained the terms "instagram," "insta," "instragram," "intagram," "inatagram," "instergram," "imstragram," or "instgram" were coded as Instagram. Next, this coding was manually reviewed and corrections made as necessary. While this manual review of the data can increase our confidence in the accuracy of the platform data reported here, there are still several limitations to bear in mind. First, review of this data indicated that complainants did not always describe *where* the content was located. Instead, this data should be considered to reflect any or all of the following: where communication initially happened between the victim and perpetrator, where or how the content was captured, where any subsequent communication occurred between the victim and perpetrator, where the content was threatened to be shared, or where the content was stored or shared. Second, in several instances the complainants did not refer to a specific platform or location. If a complainant mentioned an "app," this was coded as "Other app/app not specified"; "social media" was coded as "Social media not specified"; and "online," "internet," "google," and "google images" were coded as "Other website/website not specified." Various iterations of pornography websites, online forums, image boards, and other less commonly mentioned websites were also coded as "Other website/website not specified." Specific apps or websites mentioned in less than 50 reports across the reporting period were also coded into the aforementioned "other app"/ "other website" categories. Due to difficulty distinguishing between Facebook and Facebook Messenger in some reports, these categories were combined. Additionally, if

the platform was misspelled to a point that it could not be confidently identified, or where the complainant did not mention a specific type of platform (e.g., "direct message"), the location data was not coded. Finally, due to limited resources, we are unable to present fully disaggregated platform data and instead present aggregated categories (e.g., "Other website") for less common platforms. Therefore, findings related to location data are presented as the most common platforms *associated* with reports, should be interpreted with caution, and should be considered indicative and preliminary only.

Finally, the reporting data is not collected for research. Some details about each incident are reported by complainants using free-text fields in an online form, which are subsequently reviewed by investigators and then categorized into different variables. Data categorization is dependent on the complainant's level of understanding of terminology and how they have described the incident, and how this is interpreted by investigators, which may result in inconsistencies in reporting. There may also be inconsistencies relating to how complainants understand terms in the form. The manual nature of data entry also gives rise to the potential for data entry errors and missing data. Therefore, while the data presented in this research provides an indication of the reports received by eSafety and the experiences of complainants reporting under the IBA scheme, these limitations should be considered when interpreting the data. Further research would benefit from obtaining the perspective of complainants to the IBA scheme, to understand their experiences in reporting to the scheme.

## 5 Findings

Unless otherwise specified, the reporting period refers to reports submitted between August 18, 2018, and June 30, 2023.

### 5.1 Volume of reports and complainant demographics under eSafety's image-based abuse scheme

In the reporting period, eSafety handled 19,468 reports under Australia's IBA scheme, of which 12,221 (62.8%) involved victims who identified as male and 6,734 (34.6%) involved victims who identified as female (See Table 1 on the following page). Most victims were aged 18–24 (n = 8,515, 43.7%), and notably, almost a third of all reports involved male victims aged 18–24 (n = 6,262, 32.2%). The higher proportion of reports involving males, and the large proportion involving young males in particular, may be attributed to the significant increase in reports of sexual extortion over the reporting period (see Sections 5.3.1 and 5.5).

Table 1: Gender and age of victims who reported to the eSafety image-based abuse scheme, by financial year

| | 2018/19 | | 2019/20 | | 2020/21 | | 2021/22 | | 2022/23 | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | n | % | n | % | n | % | n | % | n | % | n | % |
| Gender | | | | | | | | | | | | |
| Female | 420 | 49.5 | 1,395 | 51.6 | 1,285 | 47.8 | 1,576 | 37.8 | 2,058 | 22.7 | 6,734 | 34.6 |
| Male | 401 | 47.2 | 1,199 | 44.4 | 1,329 | 49.4 | 2,470 | 59.2 | 6,822 | 75.3 | 12,221 | 62.8 |
| Trans/gender diverse/intersex | 6 | 0.7 | 19 | 0.7 | 17 | 0.6 | 40 | 1.0 | 44 | 0.5 | 126 | 0.6 |
| Other/prefer not to disclose | 22 | 2.6 | 89 | 3.3 | 57 | 2.1 | 83 | 2.0 | 136 | 1.5 | 387 | 2.0 |
| Age | | | | | | | | | | | | |
| under 13 | 17 | 2.0 | 44 | 1.6 | 47 | 1.7 | 82 | 2.0 | 118 | 1.3 | 308 | 1.6 |
| 13–15 | 108 | 12.7 | 308 | 11.4 | 313 | 11.6 | 510 | 12.2 | 885 | 9.8 | 2,124 | 10.9 |
| 16–17 | 88 | 10.4 | 308 | 11.4 | 329 | 12.2 | 531 | 12.7 | 960 | 10.6 | 2,216 | 11.4 |
| 18–24 | 298 | 35.1 | 1,003 | 37.1 | 1,090 | 40.6 | 1,678 | 40.2 | 4,446 | 49.1 | 8,515 | 43.7 |
| 25+ | 333 | 39.2 | 1,025 | 37.9 | 877 | 32.6 | 1,339 | 32.1 | 2,644 | 29.2 | 6,218 | 31.9 |
| Not known | 5 | 0.6 | 14 | 0.5 | 32 | 1.2 | 29 | 0.7 | 7 | 0.1 | 87 | 0.4 |
| Total | 849 | 100 | 2,702 | 100 | 2,688 | 100 | 4,169 | 100 | 9,060 | 100 | 19,468 | 100 |

Note. The Australian financial year runs from July 1 to June 30 of the following calendar year.

### 5.2 Volume of reports involving threats to share an intimate image and non-consensual sharing of an image under eSafety's image-based abuse scheme

Consistent with the large proportion of reports to eSafety of sexual extortion (see Section 5.3.1), just over three-quarters of reports (n = 14,933, 76.7%) involved victims who had received threats that their intimate images or videos would be shared online (See Table 2 on the next page). Reports regarding male victims accounted for the majority of these reports (n = 10,580, 70.8%); reports regarding female victims accounted for 26.5% (n = 3,963) of this type of report.

In comparison, less than half of reports (n = 8,914, 45.8%) involved non-consensual sharing of an image online.[6] While reports regarding male victims accounted for just over half of these reports (n = 4,759, 53.4%), among those who had reported to the scheme, female victims (n = 3,940, 58.5%) were more likely than male victims (38.9%) to request help with non-consensual image sharing. These findings indicate that men who experience IBA may be more likely to experience threats to share intimate images, whereas women may be more likely to experience the non-consensual distribution of intimate images.

Reports involving a threat to share an intimate image and those involving non-consensual sharing of an image were not mutually exclusive, with almost a quarter of reports (n = 4,467, 22.9%) involving both. More male victims (n = 3,157, 25.8%) than female victims (n = 1,213, 18.0%) reported both.

6. This includes a proportion of reports requesting help with images posted live on public-facing websites.

Table 2: Type of help requested by victims who reported to the eSafety image-based abuse scheme, by financial year

| | 2018/19 | | 2019/20 | | 2020/21 | | 2021/22 | | 2022/23 | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | n | % | n | % | n | % | n | % | n | % | n | % |
| Image that had been shared online | 395 | 46.5 | 1,066 | 39.5 | 1,262 | 46.9 | 2,127 | 51.0 | 4,064 | 44.9 | 8,914 | 45.8 |
| Image that had been threatened to be shared online | 602 | 70.9 | 2,110 | 78.1 | 1,929 | 71.8 | 3,045 | 73.0 | 7,247 | 80.0 | 14,933 | 76.7 |

### 5.3 Most common categories of behavior reported to eSafety's image-based abuse scheme

Each report to the IBA scheme is categorized by eSafety as only one type of behavior (see Table 3 on page 18). Therefore, some categories of behavior may be underrepresented in the reporting data, and the reporting categories presented here should not be considered to capture the entirety of a victim's experience. eSafety predominantly uses different categories according to the age of the victim; however, due to evolution of categories over time, in some instances certain categories of behavior have been used for both adult and minor victims. Most reports from adults (18 years old and older) were categorized as "sexual extortion," threats to share an image or non-consensual sharing of an image (categories labeled as "shared via private means," "threatened sharing," and "coercive control - posted or threatened"), or non-consensual posting of intimate images on public platforms (labeled as "posted online including on-shared monetized"). Reports to the scheme involving a minor victim (<18 years old) were predominantly categorized as "child sexual exploitation" or "peer-group sharing/threatened sharing (under 18s)." See Table 3 on page 18 for explanations of each reporting category used by eSafety.

#### 5.3.1 Sexual extortion

In the reporting period, over 6 in 10 (n = 12,098, 62.1%) reports to the eSafety IBA scheme were categorized as sexual extortion (See Table 3 on page 18). This is when someone threatens to share an intimate image unless the victim gives into their demands (e.g., for money, more intimate images, or sexual favors). Sexual extortion accounted for almost three-quarters of reports that involved a threat to share an intimate image (n = 10,982, 73.5%). Almost all (90.8%) sexual extortion reports involved a threat to share an intimate image. Sexual extortion can also result in non-consensual sharing of an image online, including sharing via private message as part of the threat and demands. Over a third (n = 4,192, 34.7%) of sexual extortion reports also involved the non-consensual sharing of an intimate image online.

Reports categorized as sexual extortion predominately involved male victims (n = 9,459, 78.2%), and most victims were aged 18–24 (n = 7,259, 60.0%) (see Table 7 on page 31). Notably, male victims aged 18–24 accounted for almost half of all sexual extortion reports (n = 6,041, 49.9%).

#### 5.3.2 Threatened sharing and non-consensual sharing of images, excluding sexual extortion

eSafety handled a smaller number of reports of threats to share an image or non-consensual sharing of an image outside of sexual extortion (See Table 3 on page 18), which were captured most frequently by reports categorized as "shared via private means" (n = 508, 2.6%), "threatened sharing" (n = 460, 2.4%), and "coercive control - posted or threatened" (n = 388, 2.0%). When combined, a similar proportion of these reports involved a threat to share an intimate image (n = 818, 60.3%), and non-consensual sharing of an image online (n = 788, 58.1%).

Victims involved in these reports were predominantly female (n = 1,071, 79.0%) and aged 25+ (n = 698, 51.5%), with female victims aged 25+ accounting for four in ten (n = 545, 40.2%) of these reports (see Table 7 on page 31). These reports are often perpetrated by partners and ex-partners or by others known to the victims, in the context of, for example, retribution or coercive control.

#### 5.3.3 Non-consensual posting of intimate images on public-facing platforms

eSafety handled fewer reports involving intimate images that had been posted without consent and were live on a public-facing platform (e.g., pornography websites). However, complaints categorized as "posted online including on-shared monetized" accounted for 5.3% (n = 1,027) of reports to eSafety's IBA scheme (See Table 3 on page 18). These reports involved intimate content, including where the original purpose was to monetize, that had been copied and posted or shared online; one example is content copied from subscription services such as OnlyFans. Most of these reports (n = 988, 96.2%) involved non-consensual sharing of an image online, and only 15.7% (n = 161) involved a threat to share an intimate image.

The majority (n = 801, 78.0%) of these reports involved female victims, and 47.5% (n = 488) of victims were aged 25+ years (see Table 7 on page 31). While females aged 25+ were the most frequent victims of this category (n = 355, 34.6%), a substantial proportion of these reports involved females aged 18–24 (n = 316, 30.8%).

#### 5.3.4 Child sexual exploitation

Almost one-quarter (n = 4,649, 23.9%) of all reports handled by eSafety were made by (or on behalf of) victims under the age of 18. Approximately six in ten (n = 2,779, 59.8%) reports involving victims under the age of 18 (14.6% of all reports) were categorized as child sexual exploitation (See Table 3 on page 18). Reports in this category refer to elicited self-generated content from a person under 18 years old and can include threats to share the content unless demands for more things, such as intimate content, money, or gift cards, are met. Perpetrators of child sexual exploitation are most often adults and are often unknown to the victim.

Most (n = 2,323, 81.9%) child sexual exploitation reports involved a threat to share an intimate image; however, there was also a large proportion (n = 1,169, 41.2%) that involved non-consensual sharing of an image online.

Overall, reports categorized as child sexual exploitation more often involved male victims (n = 1,803, 63.6%) (see Table 7 on page 31). There were slightly more child sexual exploitation reports involving older teen victims aged 16–17 (n = 1,522, 53.6%) compared with younger teens aged 13–15 (n = 1,166, 41.1%). Males aged 16–17 were the most frequent victims of child sexual exploitation reported to the scheme, accounting for almost 40% of these reports (n = 1,098, 38.7%). The large number of child sexual exploitation reports likely reflects sexual extortion scams impacting not only adult men, but also boys under the age of 18.

#### 5.3.5 Peer-group sharing (under 18s)

The other most common type of report to eSafety involving victims under the age of 18 was peer-group sharing. This is where young people under the age of 18 share or threaten to share intimate content of another young person without consent (e.g., someone they know in real life from school or a sporting club). Unlike child sexual exploitation, the person responsible for peer-group sharing is similar in age to the victim (i.e., under 18). One in six (n = 743, 16.0%) reports involving victims under the age of 18 and 3.9% of all reports handled by eSafety were categorized as peer-group sharing (See Table 3 on the following page). Peer-group sharing was associated with more reports of non-consensual sharing of an image online (n = 655, 87.1%) than threats to share an intimate image (n = 173, 23.0%).

Most reports of peer-group sharing involved victims aged 13–15 years (n = 493, 65.6%) and who identified as female (n = 554, 73.7%) (see Table 7 on page 31). Almost one in two peer-group sharing reports involved female victims aged 13–15 (n = 375, 49.9%).

Table 3: Categories of behavior reported to the eSafety image-based abuse scheme, by financial year

| | | 2018/19 | | 2019/20 | | 2020/21 | | 2021/22 | | 2022/23 | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | n | % | n | % | n | % | n | % | n | % | n | % |
| Sexual extortion | Threats to share intimate images unless demands such as payment (money, gift cards), more images, or sexual favors are met. Also includes when images have been posted online or shared via private message, as part of the threat and demands. | 432 | 50.9 | 1,662 | 61.5 | 1,541 | 57.3 | 2,276 | 54.6 | 6,187 | 68.3 | 12,098 | 62.1 |
| Posted online including on-shared monetized | Intimate content, including where the original purpose was to monetize, has been copied and posted or shared online. | 75 | 8.8 | 240 | 8.9 | 227 | 8.4 | 214 | 5.1 | 271 | 3.0 | 1,027 | 5.3 |
| Other | Reports to eSafety not otherwise captured by key categories. For example, concerns about intimate images being shared or being sent unsolicited intimate images. | 60 | 7.1 | 101 | 3.7 | 150 | 5.6 | 172 | 4.1 | 239 | 2.6 | 722 | 3.7 |
| Shared via private means | Intimate images have been shared privately and are not publicly available, such as via private message, text message or a private group chat. Not sexual extortion. | 99 | 11.7 | 123 | 4.6 | 93 | 3.5 | 93 | 2.2 | 100 | 1.1 | 508 | 2.6 |
| Threatened sharing | Received threats to share their intimate images (not sexual extortion or coercive control). Generally, the person making the threats is known. | 73 | 8.6 | 151 | 5.6 | 99 | 3.7 | 57 | 1.4 | 80 | 0.9 | 460 | 2.4 |
| Impersonation account including scam | Includes impersonation accounts that have been created purporting to sell intimate content, and where social media account/escort service is purporting to belong to victim. | 9 | 1.1 | 24 | 0.9 | 91 | 3.4 | 159 | 3.8 | 84 | 0.9 | 367 | 1.9 |
| Coercive control - posted or threatened | Received threats to share their intimate images (not sexual extortion), or images shared without consent by an ex-partner in the context of domestic and family violence. This may include threats or images shared to keep the person in the relationship; there may be history of abuse. | 6 | 0.7 | 12 | 0.4 | 84 | 3.1 | 125 | 3.0 | 161 | 1.8 | 388 | 2.0 |
| Posted or threatened sharing - intimate as without religious or cultural attire | Threat to share intimate images or intimate images have been posted online via social media posts or to websites. Images are considered “intimate” as they depict the person without religious or culture attire that they would normally wear in public. | 0 | 0.0 | 10 | 0.4 | 4 | 0.1 | 14 | 0.3 | 13 | 0.1 | 41 | 0.2 |
| Digitally altered intimate images | Intimate images purporting to be of the person. May have been digitally altered to be made to look like the person, such as their face photoshopped onto a nude image. | 3 | 0.4 | 9 | 0.3 | 9 | 0.3 | 4 | 0.1 | 14 | 0.2 | 39 | 0.2 |
| Recorded without consent | Intimate images have been captured of the person without their consent, such as a result of a hidden camera or personal recording. | 4 | 0.5 | 6 | 0.2 | 6 | 0.2 | 6 | 0.1 | 8 | 0.1 | 30 | 0.2 |
| Intimate content appearing to depict victim | Intimate content purporting to be of the person, such as a nude body image (no face showing), sent to someone along with a message naming a particular person. | 6 | 0.7 | 5 | 0.2 | <3 | n/a | <3 | n/a | 7 | 0.1 | 21 | 0.1 |
| Child sexual exploitation | Includes elicited self-generated content from a person under 18 years, and threats to a person under 18 years to share self-generated content unless demands for money, gift cards, etc. are met. | 61 | 7.2 | 298 | 11.0 | 301 | 11.2 | 770 | 18.5 | 1,407 | 15.5 | 2,837 | 14.6 |
| Peer-group sharing / threatened sharing (under 18s) | Nude content is threatened to be shared or is shared without consent between/by peers aged under 18 years, for example, between students who attended the same school or sporting club. The person responsible is a similar age to the victim, under 18. | 13 | 1.5 | 50 | 1.9 | 71 | 2.6 | 206 | 4.9 | 412 | 4.5 | 752 | 3.9 |
| Under 18s - other | All other reports to eSafety involving a victim under 18 years old. For example, when a person under 18 years may have received an unsolicited nude image, or when a person under 18 years is being impersonated. | 8 | 0.9 | 11 | 0.4 | 10 | 0.4 | 71 | 1.7 | 77 | 0.8 | 177 | 0.9 |

### 5.4 Trends in reporting to eSafety's image-based abuse scheme over time

eSafety handled a rising volume of reports under the IBA scheme, which increased by 967.1%, from 849 reports in 2018/19 to 9,060 reports in 2022/23 (Table 1 on page 14; Figure 1). In the first two financial years of the scheme, there were slightly more reports involving female victims (Table 1 on page 14; Figure 1). However, this pattern reversed in 2020/21, with a steep increase in reports involving male victims, from 2,470 in 2021/22 to 6,822 in 2022/23 (Table 1 on page 14; Figure 1). While reports involving female victims increased to a lesser extent, there was nonetheless still an increase in such reports, from 420 in 2018/19 to 2,058 in 2022/23.

In the first two financial years of the scheme, slightly more reports involved adult victims aged 25+, compared with adults aged 18–24 (Table 1 on page 14). However, again this pattern reversed in 2020/21, with a steep increase in reports regarding 18–24-year-old victims, from 1,678 in 2021/22 to 4,446 in 2022/23 (Table 1 on page 14). As described in Section 5.5, the steep increase in reports involving male victims and 18–24-year-old victims was largely driven by the increase in reports of sexual extortion.

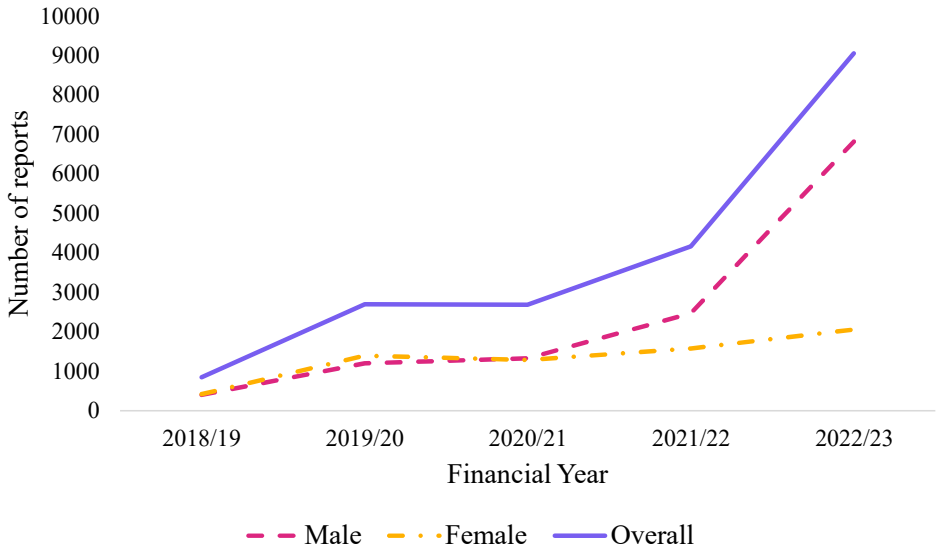


Figure 1: Change in number of reports to the eSafety image-based abuse scheme from 2018/19 to 2022/23, overall and by victim gender.

### 5.5 Trends in categories of behavior reported to eSafety's image-based abuse scheme across time

Reports categorized as sexual extortion and child sexual exploitation largely account for the rising volume of reports, which have increased by 1,332.2% (432 to 6,187; Figure 2) and 2,206.6% (61 to 1,407; Figure 3), respectively, between 2018/19 and 2022/23, and account for 76.7% (n = 14,935) of all reports in the reporting period. Again, a steep increase was observed of reports involving male victims from 2021/22 to 2022/23, for both sexual extortion (Figure 2) and child sexual exploitation (Figure 3). Reports of sexual extortion and child sexual exploitation involving female victims increased, albeit to a lesser extent, from 2018/29 to 2022/23 (see Table 7 on page 31). While there were consistently more reports of sexual extortion involving male victims, there were initially more reports of child sexual exploitation involving female victims, with this pattern reversing from 2021/22 onward (Figure 3).

Regarding age differences across time, reports categorized as sexual extortion most consistently involved 18–24-year-old victims (see Table 7 on page 31). However, there was an especially steep increase in sexual extortion reports for 18–24-year-old victims, from 1,386 in 2021/22 to 4,114 in 2022/23. There were initially slightly more reports of child sexual exploitation of 13–15-year-old victims; however, again this pattern reversed in 2021/22, with a steep increase in reports of child sexual exploitation of 16–17-year-olds, from 126 in 2020/21 to 824 in 2022/23.

While accounting for a small percentage of reports overall, there was a substantial increase in reports categorized as peer-group sharing or coercive control across the reporting period, increasing by 3,069.2% (13 to 412) and 2,583.3% (6 to 161), respectively. When considering all report categories combined, other than sexual extortion and child sexual exploitation, there was a 311.8% increase across the reporting period, with consistently more reports of these other types of behavior involving female victims (Figure 4).

### 5.6 Platforms and services associated with reports to eSafety's image-based abuse scheme

Analysis of free-text data provided by complainants when reporting to the scheme revealed that, collapsed across the reporting period, Instagram and Snapchat were the most common platforms associated with reports, with Instagram mentioned by 34.7% of complainants and Snapchat by 34% (Table 4 on the following page). Analyzing this data across the reporting period, however, revealed a shift in the most common platforms associated with reports across time. Facebook/Facebook Messenger were the most common platforms associated with reports in the first three financial years of the reporting period, while Instagram and Snapchat were more frequently mentioned by complainants from the 2021/22 financial year onward (Figure 5).

Table 4: Platforms and services associated with reports to the eSafety image-based abuse scheme from 2018/19 to 2022/23

| | 2018/19 | | 2019/20 | | 2020/21 | | 2021/22 | | 2022/23 | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | n | % | n | % | n | % | n | % | n | % | n | % |
| Instagram | 140 | 16.5 | 418 | 15.5 | 572 | 21.3 | 1,424 | 34.2 | 4,199 | 46.3 | 6,753 | 34.7 |
| Snapchat | 125 | 14.7 | 425 | 15.7 | 476 | 17.7 | 1,163 | 27.9 | 4,438 | 49.0 | 6,627 | 34.0 |
| Facebook/Facebook Messenger | 275 | 32.4 | 645 | 23.9 | 678 | 25.2 | 852 | 20.4 | 1,143 | 12.6 | 3,593 | 18.5 |
| Other websites/website not specified | 87 | 10.2 | 182 | 6.7 | 262 | 9.7 | 302 | 7.2 | 394 | 4.3 | 1,227 | 6.3 |
| WhatsApp | 54 | 6.4 | 143 | 5.3 | 204 | 7.6 | 299 | 7.2 | 488 | 5.4 | 1,188 | 6.1 |
| Email | 84 | 9.9 | 387 | 14.3 | 154 | 5.7 | 202 | 4.8 | 339 | 3.7 | 1,166 | 6.0 |
| Google Hangout/Chat/Meet | 51 | 6.0 | 197 | 7.3 | 307 | 11.4 | 320 | 7.7 | 146 | 1.6 | 1,021 | 5.2 |
| SMS/MMS | 65 | 7.7 | 118 | 4.4 | 103 | 3.8 | 113 | 2.7 | 325 | 3.6 | 724 | 3.7 |
| Kik | 28 | 3.3 | 176 | 6.5 | 114 | 4.2 | 98 | 2.4 | 69 | 0.8 | 485 | 2.5 |
| Skype | 51 | 6.0 | 123 | 4.6 | 76 | 2.8 | 94 | 2.3 | 69 | 0.8 | 413 | 2.1 |
| Discord | 3 | 0.4 | 19 | 0.7 | 23 | 0.9 | 83 | 2.0 | 183 | 2.0 | 311 | 1.6 |
| Social media not specified | 14 | 1.6 | 38 | 1.4 | 35 | 1.3 | 61 | 1.5 | 152 | 1.7 | 300 | 1.5 |
| Other apps/app not specified | 20 | 2.4 | 47 | 1.7 | 57 | 2.1 | 48 | 1.2 | 96 | 1.1 | 268 | 1.4 |
| YouTube | 30 | 3.5 | 50 | 1.9 | 57 | 2.1 | 53 | 1.3 | 82 | 0.9 | 272 | 1.4 |
| Line | <3 | n/a | 20 | 0.7 | 34 | 1.3 | 59 | 1.4 | 135 | 1.5 | 250 | 1.3 |
| Telegram | 4 | 0.5 | 7 | 0.3 | 16 | 0.6 | 51 | 1.2 | 146 | 1.6 | 224 | 1.2 |
| Twitter | 15 | 1.8 | 37 | 1.4 | 38 | 1.4 | 39 | 0.9 | 99 | 1.1 | 228 | 1.2 |
| Other dating sites/apps | 9 | 1.1 | 27 | 1.0 | 36 | 1.3 | 35 | 0.8 | 105 | 1.2 | 212 | 1.1 |
| TikTok | 0 | 0.0 | 10 | 0.4 | 19 | 0.7 | 64 | 1.5 | 108 | 1.2 | 201 | 1.0 |
| Online account | 7 | 0.8 | 12 | 0.4 | 13 | 0.5 | 15 | 0.4 | 41 | 0.5 | 88 | 0.5 |
| Pornhub | 10 | 1.2 | 44 | 1.6 | 21 | 0.8 | 6 | 0.1 | 17 | 0.2 | 98 | 0.5 |
| Reddit | 5 | 0.6 | 12 | 0.4 | 25 | 0.9 | 29 | 0.7 | 30 | 0.3 | 101 | 0.5 |
| Tinder | 6 | 0.7 | 9 | 0.3 | 11 | 0.4 | 23 | 0.6 | 39 | 0.4 | 88 | 0.5 |
| OnlyFans | 0 | 0.0 | 5 | 0.2 | 26 | 1.0 | 16 | 0.4 | 21 | 0.2 | 68 | 0.3 |
| Grindr | 7 | 0.8 | 13 | 0.5 | 10 | 0.4 | 12 | 0.3 | 16 | 0.2 | 58 | 0.3 |
| IMO | 11 | 1.3 | 13 | 0.5 | 15 | 0.6 | 14 | 0.3 | 4 | 0.0 | 57 | 0.3 |
| Omegle | 4 | 0.5 | 8 | 0.3 | 12 | 0.4 | 12 | 0.3 | 14 | 0.2 | 50 | 0.3 |

Note. Percentages do not sum to 100% as reports could be associated with more than one platform or service.

When looking at the platforms and services associated with reports of key behavior categories to eSafety's IBA scheme, there was some variation across categories (Table 5 on the following page). For example, while Instagram was the platform most commonly associated with sexual extortion reports, Snapchat was most commonly associated with child sexual exploitation reports. Snapchat was also associated with a large majority of peer-group sharing reports. Conversely, reports categorized as posted online including on-shared monetized were most commonly associated with other websites, including search engines, pornography websites, and online forums.

Table 5: Platforms and services associated with key categories of reports to the eSafety image-based abuse scheme

| | Sexual extortion | | Threatened sharing and non-consensual sharing of images (not sexual extortion) | | Posted online including on-shared monetized | | Impersonation account including scam | | Other (18+) | | Child sexual exploitation | | Peer group sharing (<18 years) | | Other (<18 years) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | n | % | n | % | n | % | n | % | n | % | n | % | n | % | n | % |
| Instagram | 4,456 | 36.8 | 264 | 19.5 | 135 | 13.1 | 239 | 65.1 | 111 | 15.4 | 1,296 | 45.7 | 167 | 22.2 | 43 | 24.3 |
| Snapchat | 3,900 | 32.2 | 323 | 23.8 | 81 | 7.9 | 23 | 6.3 | 78 | 10.8 | 1,612 | 56.8 | 534 | 71.0 | 56 | 31.6 |
| Facebook/Facebook Messenger | 2,645 | 21.9 | 378 | 27.9 | 156 | 15.2 | 42 | 11.4 | 173 | 24.0 | 130 | 4.6 | 28 | 3.7 | 16 | 9.0 |
| Other websites/website not specified | 245 | 2.0 | 100 | 7.4 | 530 | 51.6 | 115 | 31.3 | 144 | 19.9 | 45 | 1.6 | 10 | 1.3 | 18 | 10.2 |
| WhatsApp | 970 | 8.0 | 93 | 6.9 | 16 | 1.6 | <3 | n/a | 22 | 3.0 | 73 | 2.6 | 4 | 0.5 | <3 | n/a |
| Email | 938 | 7.8 | 94 | 6.9 | 26 | 2.5 | 3 | 0.8 | 39 | 5.4 | 55 | 1.9 | 5 | 0.7 | <3 | n/a |
| Google Hangout/Chat/Meet | 902 | 7.5 | 6 | 0.4 | <3 | n/a | 0 | 0.0 | 6 | 0.8 | 106 | 3.7 | 0 | 0.0 | 0 | 0.0 |
| SMS/MMS | 325 | 2.7 | 186 | 13.7 | 14 | 1.4 | <3 | n/a | 43 | 6.0 | 84 | 3.0 | 60 | 8.0 | 8 | 4.5 |
| Kik | 401 | 3.3 | 22 | 1.6 | 4 | 0.4 | 4 | 1.1 | 3 | 0.4 | 50 | 1.8 | 0 | 0.0 | 0 | 0.0 |
| Skype | 379 | 3.1 | 5 | 0.4 | <3 | n/a | <3 | n/a | 6 | 0.8 | 19 | 0.7 | <3 | n/a | <3 | n/a |
| Discord | 176 | 1.5 | 21 | 1.5 | 18 | 1.8 | <3 | n/a | 7 | 1.0 | 57 | 2.0 | 21 | 2.8 | 7 | 4.0 |
| Social media not specified | 164 | 1.4 | 30 | 2.2 | 12 | 1.2 | 7 | 1.9 | 20 | 2.8 | 41 | 1.4 | 18 | 2.4 | 4 | 2.3 |
| Other apps/app not specified | 187 | 1.5 | 27 | 2.0 | 3 | 0.3 | <3 | n/a | 11 | 1.5 | 28 | 1.0 | 6 | 0.8 | <3 | n/a |
| YouTube | 226 | 1.9 | 10 | 0.7 | 7 | 0.7 | <3 | n/a | 12 | 1.7 | 11 | 0.4 | 0 | 0.0 | 3 | 1.7 |
| Line | 244 | 2.0 | 2 | 0.1 | <3 | n/a | 0 | 0.0 | 0 | 0.0 | 3 | 0.1 | 0 | 0.0 | 0 | 0.0 |
| Telegram | 168 | 1.4 | 17 | 1.3 | 10 | 1.0 | 3 | 0.8 | <3 | n/a | 15 | 0.5 | 7 | 0.9 | 0 | 0.0 |
| Twitter | 92 | 0.8 | 22 | 1.6 | 77 | 7.5 | 3 | 0.8 | 10 | 1.4 | 20 | 0.7 | <3 | n/a | 0 | 0.0 |
| Other dating sites/apps | 170 | 1.4 | 11 | 0.8 | 6 | 0.6 | 5 | 1.4 | 4 | 0.6 | 13 | 0.5 | 0 | 0.0 | <3 | n/a |
| TikTok | 36 | 0.3 | 13 | 1.0 | 11 | 1.1 | 5 | 1.4 | 46 | 6.4 | 15 | 0.5 | 35 | 4.7 | 34 | 19.2 |
| Online account | 37 | 0.3 | 18 | 1.3 | 11 | 1.1 | 0 | 0.0 | 11 | 1.5 | 7 | 0.2 | <3 | n/a | <3 | n/a |
| Pornhub | 36 | 0.3 | 8 | 0.6 | 40 | 3.9 | <3 | n/a | 6 | 0.8 | 5 | 0.2 | 0 | 0.0 | 0 | 0.0 |
| Reddit | 16 | 0.1 | 10 | 0.7 | 62 | 6.0 | <3 | n/a | 3 | 0.4 | 5 | 0.2 | 0 | 0.0 | <3 | n/a |
| Tinder | 62 | 0.5 | 5 | 0.4 | 5 | 0.5 | 7 | 1.9 | 7 | 1.0 | <3 | n/a | 0 | 0.0 | <3 | n/a |
| OnlyFans | 5 | 0.0 | 7 | 0.5 | 23 | 2.2 | 25 | 6.8 | 8 | 1.1 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| Grindr | 22 | 0.2 | 12 | 0.9 | 5 | 0.5 | 11 | 3.0 | 6 | 0.8 | <3 | n/a | 0 | 0.0 | 0 | 0.0 |
| IMO | 54 | 0.4 | 3 | 0.2 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| Omegle | 28 | 0.2 | <3 | n/a | 0 | 0.0 | 0 | 0.0 | 3 | 0.4 | 17 | 0.6 | <3 | n/a | 0 | 0.0 |

Note. Percentages do not sum to 100% as reports could be associated with more than one platform or service. The following categories of behavior have been excluded from Table 5 due to low n's (< 50): Posted or threatened sharing - intimate as without religious or cultural attire; recorded without consent; digitally altered intimate images; intimate content appearing to depict victim.

### 5.7 Actions taken by eSafety in response to reports to the image-based abuse scheme

In addition to responding to reports to the IBA scheme with education, referrals, information, and advice, the scheme also enables eSafety to engage directly with platforms to facilitate the removal of non-consensual material.

The most common action taken by eSafety when engaging with platforms directly was to report user behavior (i.e., perpetrator accounts) to online services and platforms (Table 6 on the next page). During the reporting period, eSafety issued 9,520 reports of user behavior, with 80.0% of these reports successfully leading to removal of perpetrator accounts. Most reports of user behavior were for sexual extortion reports (55.5%), with almost 1 in 4 for child sexual exploitation reports (24.0%). Reports of user behavior were sent to 95 unique platforms and services, most commonly Instagram (35.2%), Snapchat (31.0%), and Facebook (10.7%).

In reports where intimate images have been posted on public-facing websites, the rapid removal of those images is the priority, and to respond quickly, this stream of response involves contacting the relevant website or online service on behalf of the complainant and informally requesting the removal of non-consensual images. In relation to reports received during the reporting period, eSafety sent 1,961 removal requests to 869 unique platforms and services, the majority of which were designated internet services, including pornography websites. eSafety was successful in having all or some of the material removed for 89.9% of these requests. Most removal requests were for reports categorized as “posted online including on-shared monetized” (85.1%). Among reports that had been actioned with a removal request during the reporting period, victims who identified as female requested the removal of 57 images/artifacts on average, compared with an average of 17 images/artifacts requested for removal by victims who identified as male.

When removal requests made to platforms are unsuccessful, steps are occasionally taken to “limit the discoverability” of intimate images that have been posted without consent, by having it removed from search engine results. Between 2018/19 and 2022/23, eSafety informally requested the de-indexing of search engine results in 104 instances, most commonly for reports of “posted online including on-shared monetized” (57.7%). De-indexing search results requests were most often associated with Google search results (92.4%).

Table 6: Actions taken by eSafety in response to reports of image-based abuse, by category of behavior

| | Reports of User Behavior | | Removal Requests | | De-Indexing Search Results | |
|---|---|---|---|---|---|---|
| | n | % | n | % | n | % |
| Sexual extortion | 5,283 | 55.5 | 79 | 4.0 | 3 | 2.9 |
| Child sexual exploitation | 2,284 | 24.0 | 35 | 1.8 | <3 | n/a |
| Peer group sharing / threatened sharing (under 18s) | 538 | 5.7 | 3 | 0.2 | <3 | n/a |
| Impersonation account including scam | 368 | 3.9 | 12 | 0.6 | 0 | 0.0 |
| Shared via private means | 309 | 3.2 | 28 | 1.4 | 0 | 0.0 |
| Posted online including on-shared monetized | 227 | 2.4 | 1,668 | 85.1 | 60 | 57.7 |
| Coercive control - posted or threatened | 174 | 1.8 | 87 | 4.4 | 12 | 11.5 |
| Threatened sharing | 171 | 1.8 | <3 | n/a | 0 | 0.0 |
| Other | 67 | 0.7 | 11 | 0.6 | <3 | n/a |
| Posted online or threatened sharing - intimate as without religious or cultural attire | 37 | 0.4 | <3 | n/a | 0 | 0.0 |
| Under 18s - other | 32 | 0.3 | 12 | 0.6 | 4 | 3.8 |
| Intimate content appearing to depict victim | 19 | 0.2 | 3 | 0.2 | 0 | 0.0 |
| Digitally altered intimate images | 7 | 0.1 | 20 | 1.0 | 20 | 19.2 |
| Recorded without consent | 4 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| Total | 9,520 | | 1,961 | | 104 | |

Note. One report to the IBA scheme could have been responded to with multiple actions. These figures therefore reflect the number of reports of user behavior, removal requests, and de-indexing search result requests that were actioned in relation to reports categorized as different types of behavior, as opposed to the number of reports to the scheme that were actioned with a report of user behavior, removal request, or de-indexing search result request. Additionally, not all reports to the IBA scheme result in one of these actions. eSafety also responds with education, referrals, information, and advice.

## 6 Discussion

This paper provides a descriptive overview of eSafety's IBA scheme. Examination of reporting data provided insight into complainant report trends under the scheme and insights into how eSafety responds to reports.

Both criminal and civil laws are employed within Australia and globally to respond to IBA, which come with challenges including inconsistent laws, underresourced police, evidentiary limitations, jurisdictional boundaries, and attitudes centered on harm minimization and victim blaming (Henry, Flynn, and Powell 2020). Therefore, a support system for victims to reclaim control, by removing their images, is essential. A key component of the current success and strength of eSafety's IBA scheme has been the establishment of eSafety as a centralized mechanism responsible for receiving reports (i.e., via the portal) of IBA and acting on such reports to provide support and facilitate the removal of non-consensual images. Though it is complaints-based, Australia's IBA scheme removes the onus on victims to seek out their intimate images online, to contact and report to individual platforms, and to attempt to convince platforms or users to remove the images.

This is significant given the challenges victims of IBA often experience when attempting to report their IBA content online (i.e., to platforms) (De Angeli et al. 2023) or to law enforcement (Henry, Flynn, and Powell 2018; Kolisetty 2022).

In addition, the reporting data shows that implementation of the IBA scheme has provided an increasing number of Australian victims of IBA with expert assistance and help to reclaim control, facilitate the removal of harmful content, and provide practical support to help them to feel safer online. eSafety takes a complainant-centered approach in its implementation of the IBA scheme, which includes providing information to complainants about their options and rights, including other reporting mechanisms (e.g., to the police), to empower complainants to meet their intended goals (e.g., the removal of content and/or the pursuit of criminal sanctions against perpetrators) (Yar and Drew 2019). The pursuit of criminal action against IBA perpetrators is difficult without victim reports. eSafety facilitates IBA reporting to law enforcement in cases where criminal action is desired by the complainant, and where it is necessary (e.g., reports involving complainants under the age of 16), providing complainants with a multistranded and multiagency response "that allows victims to simultaneously or consecutively pursue one or more of a number of options within and beyond the criminal justice system" (Rackley et al. 2021, 23). In summary, in the first five years of its operation, the IBA scheme has facilitated positive outcomes for victims of IBA as well as increased criminal action against perpetrators. Therefore, jurisdictions endeavoring to adopt similar IBA schemes would benefit from the establishment and provision of an accessible means through which victims can report IBA incidents.

The Online Safety Act's ultimate goal is to promote and improve the online safety of all Australians. The Explanatory Memorandum to the Act establishes that the non-consensual sharing of intimate images is a type of online harm (Parliament of Australia 2021b). When IBA is reported under the eSafety IBA scheme, there are no requirements to prove motivation or intent in the non-consensual distribution of intimate images (Parliament of Australia 2021a). The overlapping, shifting range of motivations to perpetrate IBA are acknowledged, and IBA arising across diverse contexts is captured under the scheme. Importantly, the operating model of the IBA scheme is designed to understand, prioritize, and minimize the harm associated with each report, including the threat to and invasion of privacy, and to reduce distress caused to victims. As a result, eSafety is quick to respond to victims' needs for rapid response and remedial action (i.e., content removal).

In addition, under the IBA scheme the definition of "intimate image" is not confined to those containing explicit nudity (Parliament of Australia 2021a). Rather, the scheme takes an inclusive approach, extending to diverse forms of intimate images that an individual has not chosen to share publicly, which is important given the diverse forms of intimate images and contexts of non-consensual sharing that are reported (e.g., images involving individuals without their cultural or religious attire). Further, the types of IBA that eSafety

can take action on are not limited to sharing non-consensual intimate images (Parliament of Australia 2021a). Threats to share intimate images without consent are also included under the IBA scheme. This is significant given the very high and increasing number of reports to eSafety that have involved threats to share, and the significant harm that the threat of releasing an image can cause when it is used to harass a victim or coerce them in some way (Henry, Powell, and Flynn 2017). This inclusive threshold of what constitutes IBA has facilitated an unanticipated increase in the number of reports under the scheme, especially driven by the very high proportion and increasing rates of sexual extortion and child sexual exploitation reports.

The increasing rates of sexual extortion and child sexual exploitation reported to the IBA scheme, especially reports involving young male victims, mirrors findings from international reporting data. The United Kingdom's Revenge Porn Helpline, for example, observed a 54% increase in reports of sexual extortion from 2022 to 2023, with 93% of reports of sexual extortion received in 2023 involving male victims (Papachristou 2023). Analysis of NCMEC CyberTipline data similarly showed an increase in reports of sexual extortion from 2020 to 2023, an increase largely driven by reports involving financial sexual extortion (Thorn and National Center for Missing and Exploited Children 2024). Moreover, 90% of victims of financial sexual extortion were males aged 14–17 (Thorn and National Center for Missing and Exploited Children 2024). Notably, a recent survey of 1,953 adolescents residing in Australia found that gender was not significantly associated with sexual extortion experiences, with women, men, and gender diverse adolescents reporting similar lifetime rates of sexual extortion (Wolbers et al. 2025). However, men were more likely than women to report a sexual extortion experience in the 12 months prior to the survey and were also more likely to be sexually extorted by someone they had never met in person. Moreover, men were more likely to receive financial demands from perpetrators, while women were more likely to receive demands for additional intimate material. While it was not within the scope of the present study to analyze the nature of the demands victims of sexual extortion or child sexual exploitation received, collectively, these findings point toward a surge in incidents of sexual extortion, especially financial sexual extortion, in recent years, predominantly targeting young men and boys.

While reports to the IBA scheme that were categorized as other types of behavior did not evidence as substantial an increase across the reporting period, these reports consistently involved primarily female victims. The most prevalent victim profiles observed for different categories of behavior across the reporting period may therefore suggest that men/boys and women/girls may be at heightened risk of distinct forms of IBA. While the present reporting data, combined with international reporting data (Papachristou 2023; Thorn and National Center for Missing and Exploited Children 2024), suggests that men and boys may have been at heightened risk of experiencing sexual extortion over recent years, girls and women continued to report other types of IBA more frequently than boys and men, including the threatened sharing and non-consensual sharing of

intimate images outside of sexual extortion, the non-consensual posting of intimate images on public-facing platforms, and peer-group sharing. Moreover, analysis of reports that had been actioned with a removal request during the reporting period revealed that female victims requested removal of an average of 57 images/artifacts, compared with an average of 17 for male victims. Again, this mirrors findings from international reporting data, with the United Kingdom's Revenge Porn Helpline finding that women who reported to the helpline had approximately 28 times more intimate images non-consensually shared than men (Papachristou 2023). Encouragingly, where complaints were actioned with a removal request during the reporting period, eSafety was successful in having all or some of the material removed for 89.9% of these requests.

Indeed, a key aim of the eSafety IBA scheme is to place obligations on platforms for individual pieces of harmful content. eSafety employs a predominantly informal approach in the operation of the IBA scheme, utilizing informal removal requests in the first instance. The high rates of removal in response to these requests suggests that this informal approach has been an effective means of removing harmful IBA content from platforms. This approach to facilitating platform compliance is assisted by eSafety developing and maintaining cooperative relationships with key social media and instant messaging platforms where IBA content is located. The cooperative approach is bolstered by eSafety holding trusted flagger status with key platforms, resulting in high compliance rates and a willingness to respond to informal content removal requests and reports of perpetrator accounts. This approach fast-tracks the process of content and account removal, resulting in rapid removal and a reduced burden placed on victims.

Even though platforms are typically willing to comply with the increasing number of requests from eSafety to remove content from their services, it appears that little is being done to prevent IBA from occurring and to proactively respond to IBA occurring on their platforms. Since the IBA scheme was implemented in 2018, reports have steadily increased, likely partly driven by increased prevalence and increased reporting. Increased community awareness of eSafety and the IBA scheme may have also contributed to increased reporting rates. Additionally, the reporting period includes the duration of the COVID-19 pandemic; increased time spent online during this period may have driven increased rates of IBA, and consequently increased reporting to the scheme. Notwithstanding the various potential drivers of increased reporting to the scheme, this points toward a potential disconnect between the work eSafety is doing in response to reports under the IBA scheme, and the role of platforms in proactively detecting and preventing IBA from occurring on their services. While United States-based electronic service providers are legally required to report detected instances of child sexual abuse material, including IBA, to the NCMEC CyberTipline, there are no legal requirements to proactively detect child sexual abuse material (National Center for Missing and Exploited Children, n.d.). Analysis of instances of sexual extortion of children reported to the NCMEC CyberTipline from 2020 to 2023 revealed that reports from electronic service providers constituted 85% of all reports of sexual extortion during the sampled time frame (Thorn

and National Center for Missing and Exploited Children 2024). Mirroring the present findings, Instagram, Facebook, and Snapchat were the most frequent reporters of sexual extortion of children to the NCMEC CyberTipline (Thorn and National Center for Missing and Exploited Children 2024). Instagram and Snapchat were also the most frequently mentioned platforms in public reports of sexual extortion to the NCMEC CyberTipline (Thorn and National Center for Missing and Exploited Children 2024). Notably, while Snapchat was mentioned nearly as often as Instagram in public reports, report volume directly from Snapchat to the tipline was substantially lower than that of Instagram (Thorn and National Center for Missing and Exploited Children 2024). While lower relative rates of platform reporting could be due to several reasons, these findings highlight the need for platforms to have accessible and effective reporting and moderation processes.

The stigma, shame, and embarrassment associated with IBA, however, may prevent victims from reporting their experiences (Wolak et al. 2018), and indeed the reporting numbers presented here are likely to be a significant underestimation of the prevalence of IBA in Australia, given known underreporting of the issue (Wolak et al. 2018). It is also possible that victims of IBA, particularly women and girls, may refrain from reporting such practices, due to the normalization of this kind of behavior (Ringrose, Regehr, and Whitehead 2021). Therefore, proactive detection of IBA occurring on platforms is also needed to help combat IBA or prevent it from occurring in the first place. Indeed, platforms have a responsibility to their users to take reasonable steps to address and prevent foreseeable harms on their services. By proactively detecting and preventing online harms, much of the burden for remaining safe online is shifted away from individual users and onto those most capable of identifying and addressing these harms—the service providers themselves. Technology-based detection and intervention is especially critical for IBA involving sexual extortion perpetrated by overseas criminals. Risk indicators such as the rapid creation of multiple accounts from the same device, attempts to connect (e.g., add as a friend) from users in regions linked to scamming activities, the use of commonly used images, phrases, or usernames, or attempted simultaneous contact with multiple users should alert platforms to suspicious accounts that may be used to perpetrate sexual extortion (Wolbers et al. 2025). Technology-based settings that reduce the risk of young people being contacted by strangers could also significantly reduce the prevalence of sexual extortion (Wolbers et al. 2025). While recent steps taken by companies, such as Meta limiting the extent to which younger users of Instagram have followers visible by setting their accounts to private by default, are welcome, more will need to be done to combat IBA. There are also several sites (e.g., automated scraping sites) that may never adopt such safety by design principles, and different approaches will also be required to disrupt IBA occurring on such services by, for example, targeting the companies that contract with such services to provide them with their internet connectivity.

Community awareness-raising and preventative education, as well as investment in initiatives that destigmatize and de-shame IBA and encourage help seeking, especially among those most at risk of experiencing IBA or those who may be reluctant to seek

help, will also be important in the prevention of IBA. This is especially important for emerging forms of IBA, such as sexual extortion and peer-to-peer image sharing, where there is little community awareness and understanding of the issue. Ultimately, however, responsibility and accountability for IBA primarily sits with perpetrators. While remedial directions against perpetrators may reduce recidivism and perpetration, sexual violence prevention and response work will also be critical to reducing IBA perpetration rates. Further, while eSafety is successful in removing a significant amount of IBA content hosted overseas, the transborder and cross-jurisdictional barriers between different countries could present challenges when seeking the removal of content from international platforms, particularly when dealing with smaller platforms. Given that IBA is transborder and cross-jurisdictional, even in countries with specific IBA laws, the absence of universal IBA laws makes prosecuting IBA challenging (Hall, Hearn, and Lewis 2023). Further challenges arise in cases where perpetrators of IBA reside overseas; for instance, in the recent surge of financial sexual extortion primarily targeting boys and young men, many of the perpetrators appear to be part of international organized criminal groups (Papachristou 2023; Thorn and National Center for Missing and Exploited Children 2024). Analysis of reports of financial sexual extortion of children to the NCMEC CyberTipline, for example, found that most cases were associated with organized criminal groups in Nigeria and Cote d'Ivoire (Thorn and National Center for Missing and Exploited Children 2024). Perpetrators of sexual extortion to the United Kingdom's Revenge Porn Helpline were similarly predominantly organized criminal gangs (Papachristou 2023). In cases such as these, law enforcement can be limited in their capacity to investigate and impose criminal penalties due to cross-jurisdictional and trans-geographical boundaries. Domestic and international regulation of IBA would therefore benefit from a collaborative global approach, with similar IBA reporting and removal schemes and robust legislative measures established in international jurisdictions.

Overall, the eSafety IBA scheme provides a visible and accessible mechanism through which victims can report IBA and obtain information, support, and assistance to facilitate the removal of non-consensual images. Importantly, the IBA scheme operates in a complementary manner to criminal justice responses, providing victims with a choice and allowing the pursuit of multiple outcomes, including criminal justice. Analysis of reporting data to the scheme also provides insights into the increasing prevalence and gendered forms of IBA.

## References

Australian Centre to Counter Child Exploitation. 2021. *Terminology and Definitions of Online Child Sexual Exploitation.* Accessed: 2023-03-31. https://www.accce.gov.au/sites/default/files/2021-06/Factsheet%20-%20Definitions%20of%20Online%20Child%20Sexual%20Exploitation.pdf.

Bindesbøl Holm Johansen, Katrine, Bodil Maria Pedersen, and Tine Tjørnhøj-Thomsen. 2018. "Visual Gossiping: Non-Consensual 'Nude' Sharing Among Young People in Denmark." *Culture, Health & Sexuality* 21, no. 9 (December 5, 2018): 1029–44. https://doi.org/10.1080/13691058.2018.1534140.

De Angeli, Antonella, Mattia Falduti, Maria Menendez-Blanco, and Sergio Tessaris. 2023. "Reporting Non-Consensual Pornography: Clarity, Efficiency and Distress." *Multimedia Tools and Applications* 82, no. 9 (January 17, 2023): 12829–58. https://doi.org/10.1007/s11042-022-14291-z.

Dodge, Alexa. 2023. "Looking Beyond the Law to Respond to Technology-Facilitated Violence and Bullying: Lessons Learned from Nova Scotia's CyberScan Unit." *Crime, Media, Culture* 19, no. 4 (January 4, 2023): 455–71. https://doi.org/10.1177/17416590221142762.

Dragiewicz, Molly, Delanie Woodlock, Bridget Harris, and Claire Reid. 2018. "Technology-Facilitated Coercive Control." In *The Routledge International Handbook of Violence Studies,* 244–53. Routledge. https://doi.org/10.4324/9781315270265-23.

Eaton, Asia A., Sofia Noori, Amy Bonomi, Dionne P. Stephens, and Tameka L. Gillum. 2020. "Nonconsensual Porn as a Form of Intimate Partner Violence: Using the Power and Control Wheel to Understand Nonconsensual Porn Perpetration in Intimate Relationships." *Trauma, Violence, & Abuse* 22, no. 5 (February 26, 2020): 1140–54. https://doi.org/10.1177/1524838020906533.

Eaton, Asia A., Divya Ramjee, and Jessica F. Saunders. 2022. "The Relationship Between Sextortion During COVID-19 and Pre-Pandemic Intimate Partner Violence: A Large Study of Victimization Among Diverse US Men and Women." *Victims & Offenders* 18, no. 2 (January 30, 2022): 338–55. https://doi.org/10.1080/15564886.2021.2022057.

eSafety Commissioner. 2017a. *Image-Based Abuse National Survey: Summary Report.* Research report. October. https://www.esafety.gov.au/sites/default/files/2019-07/Image-based-abuse-national-survey-summary-report-2017.pdf.

———. 2017b. *Online Portal Helps Australians Impacted by Image-Based Abuse,* October 16, 2017. https://www.esafety.gov.au/newsroom/media-releases/online-portal-helps-australians-impacted-image-based-abuse.

———. n.d. *Sexual Extortion.* Accessed: 2023-02-03. https://www.esafety.gov.au/key-issues/staying-safe/sexual-extortion.

Falduti, Mattia, and Sergio Tessaris. 2023. "Mapping the Interdisciplinary Research on Non-Consensual Pornography: Technical and Quantitative Perspectives." *Digital Threats: Research and Practice* 4, no. 3 (October 6, 2023): 1–22. https://doi.org/10.1145/3608483.

Finkelhor, David, Heather Turner, Deirdre Colburn, Kim Mitchell, and Ben Mathews. 2023. "Child Sexual Abuse Images and Youth Produced Images: The Varieties of Image-Based Sexual Exploitation and Abuse of Children." *Child Abuse & Neglect* 143 (June 17, 2023): 106269. https://doi.org/10.1016/j.chiabu.2023.106269.

Flynn, Asher, and Nicola Henry. 2019. "Image-Based Sexual Abuse: An Australian Reflection." *Women & Criminal Justice* 31, no. 4 (August 13, 2019): 313–26. https://doi.org/10.1080/08974454.2019.1646190.

Flynn, Asher, Anastasia Powell, Adrian J. Scott, and Elena Cama. 2021. "Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging Form of Image-Based Sexual Abuse." *The British Journal of Criminology* 62, no. 6 (December 3, 2021): 1341–58. https://doi.org/10.1093/bjc/azab111.

Franks, Mary Anne. 2017. "Revenge Porn Reform: A View from the Front Lines." *Florida Law Review* 69:1251. https://heinonline.org/HOL/LandingPage?handle=hein.journals/uflr69&div=43&id=&page=.

Gámez-Guadix, Manuel, Carmen Almendros, Erika Borrajo, and Esther Calvete. 2015. "Prevalence and Association of Sexting and Online Sexual Victimization Among Spanish Adults." *Sexuality Research and Social Policy* 12 (March 14, 2015): 145–54. https://doi.org/10.1007/s13178-015-0186-9.

Hall, Matthew, Jeff Hearn, and Ruth Lewis. 2023. "Image-Based Sexual Abuse: Online Gender-Sexual Violations." *Encyclopedia* 3 (1): 327–39. https://doi.org/10.3390/encyclopedia3010020.

Harris, Bridget A., and Delanie Woodlock. 2019. "Digital coercive control: Insights from two landmark domestic violence studies." *The British Journal of Criminology* 59, no. 3 (November 10, 2019): 530–50. https://doi.org/10.1093/bjc/azy052.

Haynes, Jason. 2021. "Legislative Approaches to Combating 'Revenge Porn': A Multi-jurisdictional Perspective." *Statute Law Review* 39, no. 3 (August 6, 2021): 319–36. https://doi.org/10.1093/slr/hmx008.

Henry, Nicola, and Asher Flynn. 2019. "Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support." *Violence Against Women* 25, no. 16 (July 30, 2019): 1932–55. https://doi.org/10.1177/10778012198638.

Henry, Nicola, Asher Flynn, and Anastasia Powell. 2018. "Policing Image-Based Sexual Abuse: Stakeholder Perspectives." *Police Practice and Research* 19, no. 6 (September 20, 2018): 565–81. https://doi.org/10.1080/15614263.2018.1507892.

———. 2019. “Image-Based Sexual Abuse: Victims and Perpetrators.” *Trends and Issues in Crime and Criminal Justice,* no. 572, 1–19. https://doi.org/10.52922/ti09975.

———. 2020. “Technology-Facilitated Domestic and Sexual Violence: A Review.” *Violence Against Women* 26, nos. 15-16 (October 1, 2020): 1828–54. https://doi.org/10.1177/107780121987582.

Henry, Nicola, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell, and Adrian J. Scott. 2020. *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery.* Routledge, June 10, 2020. https://doi.org/10.4324/9781351135153.

Henry, Nicola, Anastasia Powell, and Asher Flynn. 2017. *Not Just ‘Revenge Pornography’: Australians’ Experiences of Image-Based Abuse.* Research report. RMIT University, May. https://researchmgt.monash.edu/ws/portalfiles/portal/214045352/revenge_porn_report_2017.pdf.

Henry, Nicola, and Rebecca Umbach. 2024. “Sextortion: Prevalence and Correlates in 10 Countries.” *Computers in Human Behavior* 158 (May 23, 2024): 108298. https://doi.org/10.1016/j.chb.2024.108298.

Henry, Nicola, and Alice Witt. 2021. “Governing Image-Based Sexual Abuse: Digital Platform Policies, Tools, and Practices.” In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse,* 749–68. Emerald Publishing Limited, June 4, 2021. https://doi.org/10.1108/978-1-83982-848-520211054.

Internet Watch Foundation. 2024. “‘Exponential Increase in Cruelty’ as Sextortion Scams Hit Younger Victims,” August 23, 2024. https://www.iwf.org.uk/news-media/news/exponential-increase-in-cruelty-as-sextortion-scams-hit-younger-victims/.

Kolisetty, Akhila. 2022. “Gaps in the Law on Image-Based Sexual Abuse and Its Implementation: Taking an Intersectional Approach.” In *The Palgrave Handbook of Gendered Violence and Technology,* 507–27. Springer, January 1, 2022. https://doi.org/10.1007/978-3-030-83734-1_25.

Lenhart, Amanda, Michele Ybarra, and Myeshia Price-Feeney. 2016. *Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of “Revenge Porn”.* Research report. Center for Innovative Public Health Research, December 13, 2016. https://apo.org.au/sites/default/files/resource-files/2016-12/apo-nid266206.pdf.

Liggett O’Malley, Roberta, and Katelyn Smith. 2024. “Suicidal Ideation Among Male Victim-Survivors of Financial Sextortion.” *Victims & Offenders* (July 19, 2024): 1–22. https://doi.org/10.1080/15564886.2024.2379818.

Maddocks, Sophie. 2018. “From Non-Consensual Pornography to Image-Based Sexual Abuse: Charting the Course of a Problem with Many Names.” *Australian Feminist Studies* 33, no. 97 (November 1, 2018): 345–61. https://doi.org/10.1080/08164649.2018.1542592.

McGlynn, Clare, Kelly Johnson, Erika Rackley, Nicola Henry, Nicola Gavey, Asher Flynn, and Anastasia Powell. 2021. "'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse." *Social & Legal Studies* 30 (4): 541–62. https://doi.org/10.1177/0964663920947791.

McGlynn, Clare, and Erika Rackley. 2017. "Image-Based Sexual Abuse." *Oxford Journal of Legal Studies* 37 (3): 534–61. https://doi.org/10.1093/ojls/gqw033.

National Center for Missing and Exploited Children. n.d. *2023 CyberTipline Report.* Research report. Accessed: 2024-06-05. https://www.missingkids.org/cybertiplinedata.

Papachristou, Konstantinos. 2023. *Revenge Porn Helpline: 2023 Report.* Research report. Accessed: 2024-05-22. https://revengepornhelpline.org.uk/assets/documents/revenge-porn-helpline-report-2023.pdf.

Parliament of Australia. 1988. *Privacy Act 1988 (Cth).*

———. 1992. *Broadcasting Services Act 1992 (Cth).*

———. 2015a. *Enhancing Online Safety Act 2015 (Cth).*

———. 2015b. *Enhancing Online Safety for Children Act 2015 (Cth).*

———. 2018. *Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018 (Cth).*

———. 2021a. *Online Safety Act 2021 (Cth).*

———. 2021b. *Online Safety Bill 2021 - Explanatory Memorandum 2021 (Cth).*

———. 2024. *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 (Cth).*

Patchin, Justin W., and Sameer Hinduja. 2024. "The Nature and Extent of Youth Sextortion: Legal Implications and Directions for Future Research." *Behavioral Sciences & the Law* 42, no. 4 (May 22, 2024): 401–16. https://doi.org/10.1002/bsl.2667.

Patel, Unnati, and Ronald Roesch. 2022. "The Prevalence of Technology-Facilitated Sexual Violence: A Meta-Analysis and Systematic Review." *Trauma, Violence, & Abuse* 23, no. 2 (April 23, 2022): 428–43. https://doi.org/10.1177/1524838020958057.

Powell, Anastasia, and Nicola Henry. 2017. *Sexual Violence in a Digital Age.* Palgrave Macmillan London. https://doi.org/10.1057/978-1-137-58047-4.

Powell, Anastasia, Nicola Henry, and Asher Flynn. 2018. "Image-Based Sexual Abuse." In *Routledge Handbook of Critical Criminology,* 305–15. Routledge. https://doi.org/10.4324/9781315622040-28.

Powell, Anastasia, Nicola Henry, Asher Flynn, and Adrian J. Scott. 2019. "Image-Based Sexual Abuse: The Extent, Nature, and Predictors of Perpetration in a Community Sample of Australian Residents." *Computers in Human Behavior* 92 (March): 393–402. https://doi.org/10.1016/j.chb.2018.11.009.

Powell, Anastasia, Adrian J. Scott, Asher Flynn, and Nicola Henry. 2020. *Image-Based Sexual Abuse: An International Study of Victims and Perpetrators—A Summary Report.* Research report. Accessed: 2023-03-31. https://research.monash.edu/en/publications/image-based-sexual-abuse-an-international-study-of-victims-and-pe.

Powell, Anastasia, Adrian J. Scott, Asher Flynn, and Sarah McCook. 2022. "A Multi-Country Study of Image-Based Sexual Abuse: Extent, Relational Nature and Correlates of Victimisation Experiences." *Journal of Sexual Aggression* 30, no. 1 (September 5, 2022): 25–40. https://doi.org/10.1080/13552600.2022.2119292.

Rackley, Erika, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, and Anastasia Powell. 2021. "Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse." *Feminist Legal Studies* 29, no. 3 (May 27, 2021): 293–322. https://doi.org/10.1007/s10691-021-09460-8.

Reed, Lauren A., Richard M. Tolman, and L. Monique Ward. 2016. "Snooping and Sexting: Digital Media as a Context for Dating Aggression and Abuse Among College Students." *Violence Against Women* 22 (13): 1556–76. https://doi.org/10.1177/1077801216630143.

Rigotti, Carlotta, Clare McGlynn, and Franziska Benning. 2024. "Image-Based Sexual Abuse and EU Law: A Critical Analysis." *German Law Journal* (December 10, 2024): 1–22. https://doi.org/10.1017/glj.2024.49.

Ringrose, Jessica, Katilyn Regehr, and Sophie Whitehead. 2021. "'Wanna Trade?': Cisheteronormative Homosocial Masculinity and the Normalization of Abuse in Youth Digital Sexual Image Exchange." *Journal of Gender Studies* 31, no. 2 (July 5, 2021): 243–61. https://doi.org/10.1080/09589236.2021.1947206.

Ryan, David. 2018. "European Remedial Coherence in the Regulation of Non-Consensual Disclosures of Sexual Images." *Computer Law & Security Review* 34, no. 5 (September 21, 2018): 1053–76. https://doi.org/10.1016/j.clsr.2018.05.016.

Schmidt, Felipa, Filippo Varese, Amanda Larkin, and Sandra Bucci. 2024. "The Mental Health and Social Implications of Nonconsensual Sharing of Intimate Images on Youth: A Systematic Review." *Trauma, Violence, & Abuse* 25, no. 3 (July 25, 2024): 2158–72. https://doi.org/10.1177/15248380231207896.

Scott, Adrian J., Chelsea Mainwaring, Asher Flynn, Anastasia Powell, and Nicola Henry. 2022. "The Extent and Nature of Image-Based Sexual Abuse Among Australian Youths: Perspectives from Victims, Perpetrators and Bystanders." In *Interpersonal Violence Against Children and Youth,* 85–108. Lexington Books. https://research.gold.ac.uk/id/eprint/29363/.

Semenzin, Silvia, and Lucia Bainotti. 2020. "The Use of Telegram for Non-Consensual Dissemination of Intimate Images: Gendered Affordances and the Construction of Masculinities." *Social Media + Society* 6, no. 4 (December 29, 2020): 2056305120984453. https://doi.org/10.1177/2056305120984453.

Stevenson-McCabe, Seonaid, and Sarai Chisala-Tempelhoff. 2021. "Image-Based Sexual Abuse: A Comparative Analysis of Criminal Law Approaches in Scotland and Malawi." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse,* 513–32. Emerald Publishing Limited, June 4, 2021. https://doi.org/10.1108/978-1-83982-848-520211038.

Stokes, Jenna K. 2015. "The Indecent Internet: Resisting Unwarranted Internet Exceptionalism Combating Revenge Porn." *Berkeley Technology Law Journal* 29 (April 15, 2015): 929. https://heinonline.org/HOL/LandingPage?handle=hein.journals/berktech29&div=27&id=&page=.

StopNCII.org. n.d. *Stop Non-Consensual Intimate Image Abuse.* Accessed: 2023-03-20. https://stopncii.org/.

Thorn and National Center for Missing and Exploited Children. 2024. *Trends in Financial Sextortion: An Investigation of Sextortion Reports in NCMEC CyberTipline Data.* Research report. Accessed: 2024-06-24. June 24, 2024. https://www.thorn.org/research/library/financial-sextortion/.

Umbach, Rebecca, Nicola Henry, Gemma Faye Beard, and Colleen M. Berryessa. 2024. "Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries." In *Proceedings of the CHI Conference on Human Factors in Computing Systems,* 779:1–20. Association for Computing Machinery, May 11, 2024. https://doi.org/10.1145/3613904.3642382.

van de Weijer, Steve G. A., Rutger Leukfeldt, and Wim Bernasco. 2018. "Determinants of Reporting Cybercrime: A Comparison Between Identity Theft, Consumer Fraud, and Hacking." *European Journal of Criminology* 16, no. 4 (May 19, 2018): 486–508. https://doi.org/10.1177/1477370818773610.

Wolak, Janis, David Finkelhor, Wendy Walsh, and Leah Treitman. 2018. "Sextortion of Minors: Characteristics and Dynamics." *Journal of Adolescent Health* 62 (1): 72–79. https://doi.org/10.1016/j.jadohealth.2017.08.014.

Wolbers, Heather, Timothy Cubitt, Michael Cahill, Sarah Napier, Mariesa Nicholas, Melanie Burton, and Katherine Giunta. 2025. "Sexual Extortion Among Australian Adolescents: Results from a National Survey." *Trends & Issues in Crime and Criminal Justice* 712 (February 20, 2025). https://doi.org/10.52922/ti77819.

Yar, Majid, and Jacqueline Drew. 2019. "Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales." *International Journal of Cyber Criminology* 13 (2): 578–94. https://doi.org/10.5281/zenodo.3709306.

## Authors

**Melanie Burton** (Melanie.Burton@eSafety.gov.au) is a Senior Research Officer at the eSafety Commissioner.
**Savannah Minihan** is a Research Officer at the eSafety Commissioner.
**Mariesa Nicholas** is the Research and Evaluation Manager at the eSafety Commissioner.
**Jason Connor** is the Digital Business and Data Services Manager at the eSafety Commissioner.
**Kylie Trengove** is a Senior Research Officer at the eSafety Commissioner.

## Acknowledgements

We acknowledge our colleagues at the eSafety Commissioner who reviewed and supported this research. We also acknowledge eSafety's Image-Based Abuse team for the work they do supporting and assisting victim-survivors of image-based abuse.

## Data availability statement

Not applicable.

## Funding statement

This research was funded by the Australian government through the eSafety Commissioner. All authors are employees of the Australian Communications and Media Authority (ACMA) working under the direction of the eSafety Commissioner.

## Ethical standards

Not applicable.

## Keywords

Image-based abuse; non-consensual sharing of images; regulatory scheme; reporting; Australia; Online Safety Act; online abuse.

# Appendices

## Appendix A: Gender and age of victims reporting to eSafety's image-based abuse scheme under key reporting categories

Table 7: Gender and age of victims reporting to the eSafety image-based abuse scheme under key reporting categories, by financial year.

| | 2018/19 | | 2019/20 | | 2020/21 | | 2021/22 | | 2022/23 | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | n | % | n | % | n | % | n | % | n | % | n | % |
| **Sexual extortion** | | | | | | | | | | | | |
| Female | 105 | 24.3 | 608 | 36.6 | 440 | 28.6 | 468 | 20.6 | 708 | 11.4 | 2,329 | 19.3 |
| Male | 314 | 72.7 | 978 | 58.8 | 1,051 | 68.2 | 1,739 | 76.4 | 5,377 | 86.9 | 9,459 | 78.2 |
| under 13 | 0 | 0.0 | 3 | 0.2 | <3 | n/a | <3 | n/a | 4 | 0.1 | 10 | 0.1 |
| 13–15 | 9 | 2.1 | 38 | 2.3 | 45 | 2.9 | 5 | 0.2 | 6 | 0.1 | 103 | 0.9 |
| 16–17 | 24 | 5.6 | 104 | 6.3 | 128 | 8.3 | 10 | 0.4 | 8 | 0.1 | 274 | 2.3 |
| 18–24 | 218 | 50.5 | 745 | 44.8 | 796 | 51.7 | 1,386 | 60.9 | 4,114 | 66.5 | 7,259 | 60.0 |
| 25+ | 180 | 41.7 | 764 | 46.0 | 555 | 36.0 | 857 | 37.7 | 2,051 | 33.2 | 4,407 | 36.4 |
| **Threatened sharing and non-consensual sharing of images (not sexual extortion)** | | | | | | | | | | | | |
| Female | 140 | 78.7 | 219 | 76.6 | 225 | 81.5 | 221 | 80.4 | 266 | 78.0 | 1,071 | 79.0 |
| Male | 35 | 19.7 | 56 | 19.6 | 50 | 18.1 | 50 | 18.2 | 71 | 20.8 | 262 | 19.3 |
| under 13 | 4 | 2.2 | 4 | 1.4 | 5 | 1.8 | <3 | n/a | <3 | n/a | 15 | 1.1 |
| 13–15 | 33 | 18.5 | 30 | 10.5 | 26 | 9.4 | 10 | 3.6 | 7 | 2.1 | 106 | 7.8 |
| 16–17 | 24 | 13.5 | 35 | 12.2 | 24 | 8.7 | 5 | 1.8 | 8 | 2.3 | 96 | 7.l |
| 18–24 | 38 | 21.3 | 103 | 36.0 | 87 | 31.5 | 94 | 34.2 | 110 | 32.3 | 432 | 31.9 |
| 25+ | 78 | 43.8 | 112 | 39.2 | 130 | 47.1 | 163 | 59.3 | 215 | 63.0 | 698 | 51.5 |
| **Posted online including on-shared monetized** | | | | | | | | | | | | |
| Female | 56 | 74.7 | 187 | 77.9 | 184 | 81.1 | 168 | 78.5 | 206 | 76.0 | 801 | 78.0 |
| Male | 15 | 20.0 | 49 | 20.4 | 40 | 17.6 | 39 | 18.2 | 56 | 20.7 | 199 | 19.4 |
| under 13 | 0 | 0.0 | 5 | 2.1 | <3 | n/a | 0 | 0.0 | <3 | n/a | 8 | 0.8 |
| 13–15 | 8 | 10.7 | 28 | 11.7 | 14 | 6.2 | 15 | 7.0 | 4 | 1.5 | 69 | 6.7 |
| 16–17 | 7 | 9.3 | 22 | 9.2 | 17 | 7.5 | 6 | 2.8 | 15 | 5.5 | 67 | 6.5 |
| 18–24 | 22 | 29.3 | 93 | 38.8 | 99 | 43.6 | 80 | 37.4 | 91 | 33.6 | 385 | 37.5 |
| 25+ | 35 | 46.7 | 88 | 36.7 | 93 | 41.0 | 113 | 52.8 | 159 | 58.7 | 488 | 47.5 |

*Continued on next page*

*Continued from previous page*

| | 2018/19 | | 2019/20 | | 2020/21 | | 2021/22 | | 2022/23 | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | n | % | n | % | n | % | n | % | n | % | n | % |
| **Impersonation account including scam** | | | | | | | | | | | | |
| Female | 4 | 44.4 | 18 | 75.0 | 76 | 83.5 | 148 | 93.1 | 75 | 89.3 | 321 | 87.5 |
| Male | 4 | 44.4 | 5 | 20.8 | 12 | 13.2 | 10 | 6.3 | 9 | 10.7 | 40 | 10.9 |
| under 13 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | <3 | n/a | 0 | 0.0 | <3 | n/a |
| 13–15 | 0 | 0.0 | <3 | n/a | 6 | 6.6 | 9 | 5.7 | <3 | n/a | 18 | 4.9 |
| 16–17 | 0 | 0.0 | <3 | n/a | 14 | 15.4 | 8 | 5.0 | 6 | 7.1 | 30 | 8.2 |
| 18–24 | 4 | 44.4 | 11 | 45.8 | 41 | 45.1 | 69 | 43.4 | 38 | 45.2 | 163 | 44.4 |
| 25+ | 5 | 55.6 | 10 | 41.7 | 26 | 28.6 | 66 | 41.5 | 37 | 44.0 | 144 | 39.2 |
| **Other (18+)** | | | | | | | | | | | | |
| Female | 40 | 66.7 | 73 | 72.3 | 106 | 70.7 | 114 | 66.3 | 151 | 63.2 | 484 | 67.0 |
| Male | 16 | 26.7 | 24 | 23.8 | 36 | 24.0 | 50 | 29.1 | 74 | 31.0 | 200 | 27.7 |
| under 13 | 6 | 10.0 | 6 | 5.9 | 8 | 5.3 | 5 | 2.9 | 8 | 3.3 | 33 | 4.6 |
| 13–15 | 13 | 21.7 | 12 | 11.9 | 12 | 8.0 | 8 | 4.7 | 10 | 4.2 | 55 | 7.6 |
| 16–17 | 4 | 6.7 | 11 | 10.9 | 10 | 6.7 | 4 | 2.3 | 5 | 2.1 | 34 | 4.7 |
| 18–24 | 10 | 16.7 | 30 | 29.7 | 56 | 37.3 | 30 | 17.4 | 65 | 27.2 | 191 | 26.5 |
| 25+ | 27 | 45.0 | 42 | 41.6 | 61 | 40.7 | 120 | 69.8 | 151 | 63.2 | 401 | 55.5 |
| **Child sexual exploitation** | | | | | | | | | | | | |
| Female | 48 | 78.7 | 219 | 73.5 | 179 | 59.5 | 237 | 30.8 | 268 | 19.0 | 951 | 33.5 |
| Male | 10 | 16.4 | 68 | 22.8 | 115 | 38.2 | 507 | 65.8 | 1,103 | 78.4 | 1,803 | 63.6 |
| under 13 | 4 | 6.6 | 14 | 4.7 | 19 | 6.3 | 29 | 3.8 | 25 | 1.8 | 91 | 3.2 |
| 13–15 | 30 | 49.2 | 161 | 54.0 | 148 | 49.2 | 286 | 37.1 | 541 | 38.5 | 1,166 | 41.1 |
| 16–17 | 22 | 36.1 | 110 | 36.9 | 126 | 41.9 | 440 | 57.1 | 824 | 58.6 | 1,522 | 53.6 |
| 18–24 | 4 | 6.6 | 12 | 4.0 | 7 | 2.3 | 12 | 1.6 | 16 | 1.1 | 51 | 1.8 |
| 25+ | <3 | n/a | <3 | n/a | 0 | 0.0 | <3 | n/a | <3 | n/a | 5 | 0.2 |
| **Peer-group sharing (<18 years)** | | | | | | | | | | | | |
| Female | 9 | 69.2 | 45 | 90.0 | 52 | 73.2 | 150 | 72.8 | 298 | 72.3 | 554 | 73.7 |
| Male | 4 | 30.8 | 5 | 10.0 | 19 | 26.8 | 53 | 25.7 | 109 | 26.5 | 190 | 25.3 |
| under 13 | <3 | n/a | 11 | 22.0 | 9 | 12.7 | 22 | 10.7 | 53 | 12.9 | 96 | 12.8 |
| 13–15 | 8 | 61.5 | 24 | 48.0 | 53 | 74.6 | 135 | 65.5 | 273 | 66.3 | 493 | 65.6 |
| 16–17 | 4 | 30.8 | 13 | 26.0 | 9 | 12.7 | 46 | 22.3 | 81 | 19.7 | 153 | 20.3 |
| 18–24 | 0 | 0.0 | <3 | n/a | 0 | 0.0 | 3 | 1.5 | 4 | 1.0 | 9 | 1.2 |

*Continued on next page*

*Continued from previous page*

| | 2018/19 | | 2019/20 | | 2020/21 | | 2021/22 | | 2022/23 | | Total | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | n | % | n | % | n | % | n | % | n | % | n | % | |
| 25+ | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | |
| Other (< 18 years) | | | | | | | | | | | | | |
| Female | 6 | 75.0 | 7 | 63.6 | 7 | 70.0 | 48 | 67.6 | 46 | 59.7 | 114 | 64.4 | |
| Male | <3 | n/a | 4 | 36.4 | <3 | n/a | 18 | 25.4 | 21 | 27.3 | 47 | 26.6 | |
| under 13 | <3 | n/a | 0 | 0.0 | 4 | 40.0 | 18 | 25.4 | 25 | 32.5 | 48 | 27.1 | |
| 13–15 | 4 | 50.0 | 5 | 45.5 | 6 | 60.0 | 41 | 57.7 | 38 | 49.4 | 94 | 53.1 | |
| 16–17 | <3 | n/a | 5 | 45.5 | 0 | 0.0 | 10 | 14.1 | 12 | 15.6 | 29 | 16.4 | |
| 18–24 | <3 | n/a | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | <3 | n/a | |
| 25+ | 0 | 0.0 | <3 | n/a | 0 | 0.0 | <3 | n/a | <3 | n/a | 4 | 2.3 | |

Note. Due to evolution of reporting categories over time, in some instances certain categories of behavior have been used for both adult and minor victims. The following categories of behavior have been excluded from Table 7 due to low n's (< 50): Posted or threatened sharing - intimate as without religious or cultural attire; recorded without consent; digitally altered intimate images; intimate content appearing to depict victim.

## Appendix B: Trends in categories of behavior reported to eSafety's image-based abuse scheme across time

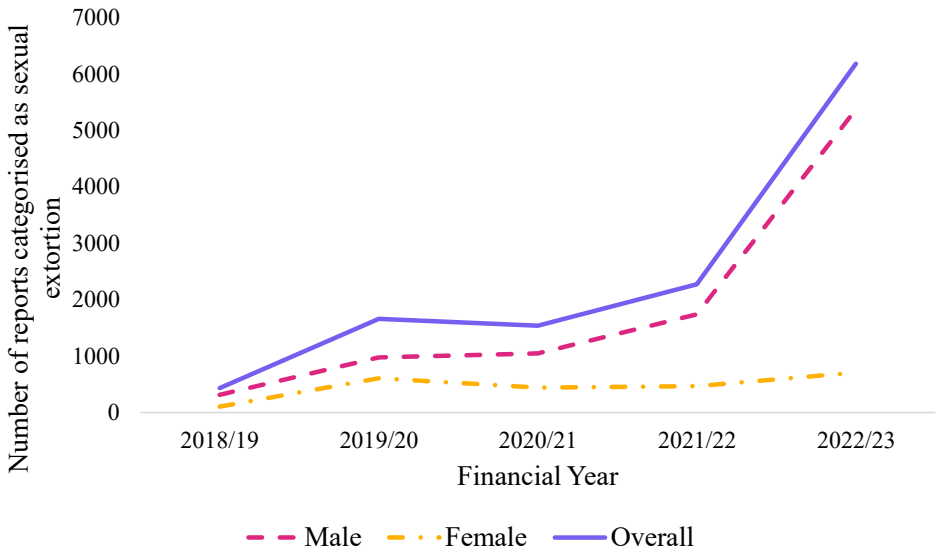


Figure 2: Change in number of reports to the eSafety image-based abuse scheme categorized as sexual extortion from 2018/19 to 2022/23, overall and by victim gender.

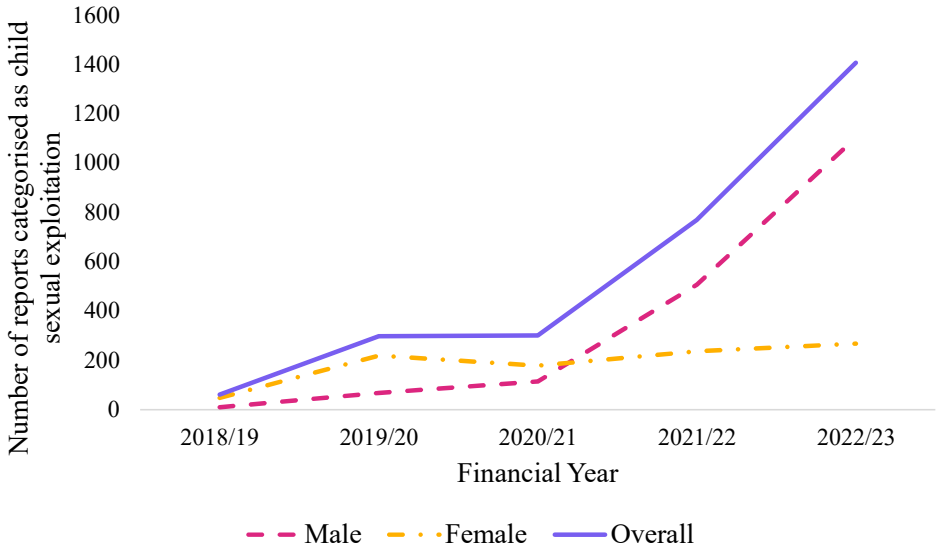


Figure 3: Change in number of reports to the eSafety image-based abuse scheme categorized as child sexual exploitation from 2018/19 to 2022/23, overall and by victim gender.

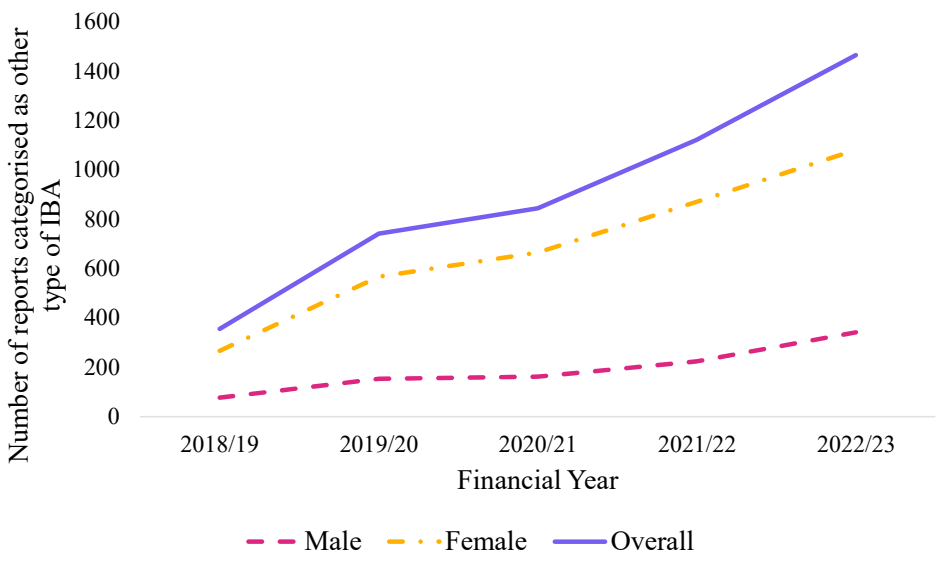


Figure 4: Change in number of reports to the eSafety image-based abuse scheme categorized as other types of behavior from 2018/19 to 2022/23, overall and by victim gender.

Note. "Other types of behavior" includes reports categorized as posted online including on-shared monetized; peer group sharing/threatened sharing – under 18s; shared via private means; threatened sharing; coercive control – posted or threatened; impersonation account – including spam; posted online or threatened sharing – intimate as without religious or cultural attire; digitally altered intimate images; recorded without consent; intimate content appearing to depict victim; other; under 18s – other. Does not include reports categorized as sexual extortion or child sexual exploitation.

## Appendix C: Platforms and services associated with reports to eSafety's image-based abuse scheme

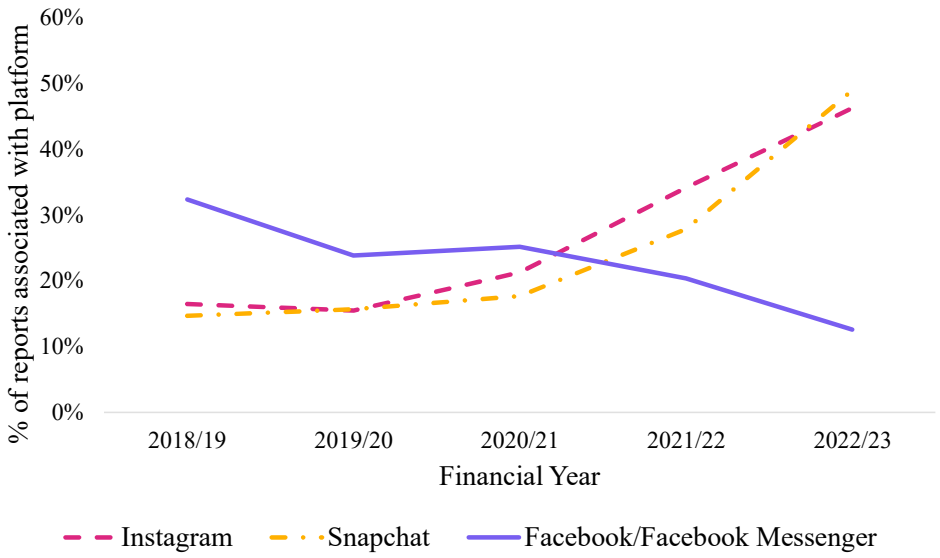


Figure 5: Most common platforms associated with reports to the eSafety image-based abuse scheme from 2018/19 to 2022/23.