TECHLEGALITY

SASHA SAFE SHARE TECHNOLOGY

HUMAN RIGHTS IMPACT ASSESSMENT

EXECUTIVE SUMMARY

I. INTRODUCTION

SASHA (short for 'Safe Share') is a Danish social impact technology company founded in 2020 that seeks to prevent and address online image-based abuse (IBA) and identity theft. **SASHA's business aim is to empower and support victim-survivors[1] to take back control over their images and to hold perpetrators legally accountable for their actions.**

SASHA is developing cutting edge technology to help victim-survivors have their images removed if shared non-consensually, and to prevent the sharing of non-consensual images in the first place. The product is currently in development stage. SASHA aims to deploy its product at scale within Europe and North America, and ultimately globally.

1 Tech Legality uses the term victim-survivor to acknowledge the potential ongoing effects and harm caused by technology-facilitated abuse and violence as well as honouring the strength and resilience of people with lived experience of technology-facilitated abuse and violence.

While the SASHA product clearly contributes to the enjoyment of human rights of victim-survivors by helping them to seek justice for the rights violations they suffered, SASHA want to ensure that their product does not also inadvertently adversely impact the human rights of victim-survivors, users and the general population, particularly the most vulnerable communities.

A key concern internationally relates to the identification and removal of IBA without negatively impacting freedom of expression or developing technology that results in infringements of the right to privacy, amongst other human rights.

It is against this background that SASHA engaged Tech Legality, a consultancy firm specialising in human rights and digital technologies, to carry out an independent human rights impact assessment (HRIA) of the SASHA product.

The objectives of this HRIA are to:

1) Analyse the role SASHA's product could play in preventing and responding to IBA and identity theft through a human rights lens;

2) Identify potential adverse human rights impacts and make recommendations to prevent or mitigate those, including risks to SASHA's users and others impacted by SASHA's products, in particular vulnerable groups;

3) Determine how SASHA can best formulate its company governance structure and company grievance mechanisms before the product is deployed in the market.

II. METHODOLOGY

This HRIA is based on the methodology of the **UN Guiding Principles on Business and Human Rights**, together with guidance from the **UN Human Rights B-Tech project**, and from the **Danish Institute for Human Rights on the operationalisation of the UNGPs in the digital environment**. It also draws on the **Global Network Initiative (GNI) Principles on Freedom of Expression and Privacy** which provide high-level guidance to the technology industry on how to respect, protect, and advance users' rights to freedom of expression and privacy when faced with government demands or restrictions.

Carrying out a HRIA is part of the human rights due diligence process. SASHA's product is currently still in the development phase. **Embarking on human rights due diligence during the product development phase is best practice, because many adverse impacts on human rights can be identified, prevented, or mitigated before the product is deployed.**

The HRIA was conducted in various stages, starting with research and scoping and followed by comprehensive stakeholder engagement. Tech Legality carried out key informant interviews with rightsholders and their proxies across a range of disciplines and geographies. This included digital rights experts, human rights defenders, and IBA experts from eight different jurisdictions (Australia, Chile, Italy, Kenya, Netherlands, Norway, United Kingdom, United States), focusing on stakeholders with heightened risk of vulnerability. Based on the primary and secondary data gathered and analysed, Tech Legality conducted the HRIA.

The HRIA was carried out between March and July 2024 and was led by Tech Legality's co-founders Emma Day and Sabine K Witting, supported by Tech Legality's consultant human rights lawyers Louise Hooper and Valentina Vivallo Toro. Tech Legality conducted this HRIA independently, maintaining editorial control over its content.

Potential human rights impacts have been analysed in accordance with international and European human rights law, focusing on the international and European human rights instruments:

- **Convention Against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment (CAT)**
- **Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)**
- **Convention on the Rights of Persons with Disabilities (CRPD)**
- **Convention on the Rights of the Child (CRC)**
- **European Charter on Fundamental Rights (CFR)**
- **European Convention on Human Rights (ECHR)**
- **International Convention on the Elimination of All Forms of Racial Discrimination (ICERD)**
- **International Covenant on Civil and Political Rights (ICCPR)**
- **International Covenant on Economic, Social and Cultural Rights (ICESCR)**
- **Universal Declaration of Human Rights (UDHR)**

III. PRODUCT DESCRIPTION

The SASHA technology caters for two different models, a business-to-consumer (B2C) and a business-to-business-to-consumer (B2B2C) model. SASHA is currently concentrating on the B2C model, but its ultimate goal is the B2B2C model which will make the B2C model redundant.

B2C MODEL

For the B2C model, SASHA is developing an App which allows users to catalogue images as the property of the creator of an image on device-level. For this purpose, SASHA uses a combination of different technologies, including Artificial Intelligence (AI) (hereafter referred to as SASHA technology). Importantly, SASHA does not have access to or store the original image. This aims to guarantee the highest level of privacy to SASHA users.

Users can share their catalogued images through the App. **If another user tries to share an image through the SASHA App, SASHA uses its technology to see whether this particular image file is a derivative of an image file explicitly marked as "not shareable" by another user. In this case the SASHA App blocks the share.**

When setting up an account on the SASHA App, SASHA aims to verify the user's identity through a third-party system. If disputes over image ownership occur, SASHA aims to partner with sponsors and law firms to ensure that every user has legal representation to settle such disputes. For this purpose, the SASHA App will compile an evidence package for the affected user to be able to prove ownership. The first step for legal action is to use the evidence package to ask the platform to take down the images. If the platforms fail to act, SASHA aims to assist the user to sue the platform for compensation and force take-down of the image or even help users with class actions against platforms.

B2B2C MODEL

The B2B2C model aims to integrate the SASHA technology on both device and platform level. The integration of the technology on device level enables the automatic cataloguing of every image or video that is taken on the device. As with the B2C model, SASHA will not store the images themselves to preserve the privacy of the users.

The B2B2C model aims to not only make it easier for victim-survivors to identify a perpetrator of non-consensual image sharing, but to prevent such non-consensual sharing in the first place. Through partnerships, SASHA aims to integrate its technology directly on platform level. Every image which is uploaded on a partner platform will be checked on device level. If the image is catalogued by SASHA technology, and the person uploading the image does not hold copyright according to the SASHA database, the upload will be blocked and – if the platform opts to do so - the owner of the image is notified of the attempted upload.

IV. SALIENT HUMAN RIGHTS RISKS

IV.1 DATA PROTECTION

ANALYSIS

As the SASHA App (B2C model) is still in development stage, and the exact details of the B2B2C model are not conceptualised yet, it cannot be comprehensively assessed how the SASHA product under both business models might impact the protection of an individual's data. This will largely depend on which type of data is collected and by whom for which purpose, how it is processed and on what legal basis and how sensitive data is being dealt with. Consideration must be given to both the person uploading an image, the person receiving an image and any subsequent individual who is sent the image. SASHA must also pay specific attention to ensure high levels of data security, i.e. protecting data from unauthorised access, disclosure, alteration and loss.

- Users might not fully understand when and how the SASHA technology is operating on their device. Regarding the B2B2C model, it will be crucial to determine how device users can control whether and how the SASHA technology is enabled on their device, e.g. by providing an opt-in or an opt-out mechanism.

- Further, the database created by SASHA may create new opportunities for surveillance. SASHA aims to build a data base which can be a powerful tool to identify individuals. SASHA will be especially effective at identifying individuals if the B2B2C model is successful in integrating the SASHA technology on device level.

- There is a risk that governments will approach SASHA with requests for specific user data, either under national laws which may not always comply with international human rights law, or by informal requests where there is no legal basis, but nonetheless considerable pressure exerted.

- These cases might be exacerbated where data requested or acquired concerns a user who is particularly vulnerable, e.g. a user from an LGBTIQ+ community or a female user in a cultural context where LGBTIQ+ or female sexual expression is condemned or even illegal.

HUMAN RIGHTS IMPACTS

- SASHA's practice of collecting, processing and sharing data might adversely impact the right to privacy (Art 12 UDHR, Art 17 ICCPR, Art 16 CRC, Art 8 ECHR) and their right to data protection (Art 8 CFR), depending on the lawfulness of the data protection practice and whether SASHA adheres to data protection principles.

- Where the information is used for criminal prosecutions, e.g. for same-sex sexual activity, this impacts the right to life (Art 3 UDHR, Art 6 (1) ICCPR, Art 2 ECHR, Art 2 CFR, Art 6 CRC) in countries where the death penalty is used; torture, inhuman or degrading treatment (CAT and Art 5 UDHR, Art 7 ICCPR, Art 3 ECHR, Art 4 CFR, Art 37 (a) CRC).

- This might also have a chilling effect on freedom of expression (Art 19 UDHR, Art 19 ICCPR, Art 10 ECHR, Art 11 CFR, Art 13 CRC), as platform users might be scared to be accused of a criminal offence and hence not freely engage in legitimate speech anymore.

IV.2 PRIVACY

ANALYSIS

Under the B2B2C model, SASHA aims to work with platforms to integrate their technology on platform level, enabling platforms to scan images and block unauthorised upload.

- Voluntary detection measures by platforms to detect illegal material on public platforms are usually permitted under different legal frameworks. However, the question is how the platform, once the material has been flagged with the use of SASHA technology, determines the illegality of the content, as the images are only considered illegal if they are shared non-consensually (unless they are sexual images of children). Further, the processing of personal data for the purpose of content blocking or removal must be lawful. As these images might be sexual in nature and constitute sensitive data, a higher threshold for data protection compliance might apply.

- **The issue of upload filters becomes more complex if the filters, powered by SASHA technology, are intended to be deployed in private communications.** Private communications enjoy a high level of protection under international human rights law, and their general monitoring – even if done voluntarily - is only permissible in narrow circumstances, for example with the explicit and informed consent of the user or if mandated by law.

- It is important to note that the SASHA technology does not function in end-to-end encrypted (E2EE) environments. Technical measures to screen the content of messages in E2EE systems introduce systemic risks for both service providers and users. To be able to detect non-consensual images in E2EE communications, SASHA would need to work with the platform to set up a system of client-side-scanning, i.e. scanning the content on device level before the content is shared in the E2EE environment. Client-side scanning would compromise the integrity of devices and systems, leaving them open to system-wide attacks, as well as malicious and accidental breaches of personal data. Alternatively, the platform would have to build in backdoor access to allow for the decryption of targeted content. **In 2024, the European Court of Human Rights concluded that decrypting end-to-end encrypted communications would inevitably result in a compromised encryption system for all users, rendering such measures not proportionate to the legitimate aims pursued, see case of Podchasov v. Russia.**

HUMAN RIGHTS IMPACTS

- The scanning of content before upload on public platforms might adversely impact the right to data protection and the right to privacy (Art 12 UDHR, Art 17 ICCPR, Art 16 CRC, Art 8 ECHR, Art 7 CFR; right to protection of personal data, Art 8 CFR). This is further exacerbated if the SASHA technology is deployed to scan content in private messages on platform level, and even more so if scanning takes place on device level (client-side scanning) or through backdoor access, as such technical measures introduce systemic risks for both service provider and users.

- Depending on the means the platform deploys to determine illegality, the use of the SASHA technology might also contribute to a chilling effect on freedom of expression (Art 19 UDHR, Art 19 ICCPR, Art 10 ECHR, Art 11 CFR, Art 13 CRC), as platform users might be scared to be accused of a criminal offence and hence not freely engage in legitimate speech anymore.

IV.3 USE OF THE PRODUCT IN MORE AUTHORITARIAN COUNTRIES

ANALYSIS

The SASHA technology has been designed with the intention that adult users can use it as an avenue to safely share images, including sexual images, while protecting their images from unwanted onward sharing.

- In most jurisdictions it is not illegal for adults to share intimate images of themselves. However, in some jurisdictions where all pornography is illegal (for example China, South Korea, Vietnam, Uganda, Tanzania), **adults may risk prosecution for this where their own sexual images taken for personal use are deemed to be self-produced pornography.**

- In an increasing number of jurisdictions (e.g. Ghana, Malaysia, Bangladesh, Pakistan) homosexuality is criminalised, and this means that where SASHA users who are LGBTQ+ share intimate images of themselves, they may risk leaving an evidence trail related to their production of materials that are deemed illegal under national laws.

In these cases, the SASHA technology could be used to identify specific users for the purpose of a criminal investigation.

As with many kinds of technology, there is always a risk of mission creep. SASHA's technology is targeted at IBA and identity theft as primary use cases. However, SASHA has no control over what type of images are catalogued through the SASHA App. The SASHA technology could therefore be used for any kind of copyright and image claiming, including journalistic photos, political photos etc.

- This might make SASHA a suitable tool for censorship, whereby bad actors, including governments and political parties, claim images for themselves which they do not want to be in circulation, e.g. pictures of a protest or pictures of war crimes. If users try to upload these images on platforms who have partnered with SASHA, the upload of the image will be automatically blocked and its dissemination hindered.

HUMAN RIGHTS IMPACTS

- In cases where SASHA users are identified as having produced pornography which is illegal under national law, this could lead to a violation of their right to privacy (Art 12 UDHR, Art 17 ICCPR, Art 16 CRC, Art 8 ECHR, Art 7 CFR) and their right to liberty and security of the person (Art 3 UDHR, Art 9 (1) ICCPR, Art 5 (1) ECHR, Art 6 CFR, Art 37 (b) CRC) if they are subsequently prosecuted for this.

- If bad actors such as governments and political parties use the SASHA product for censorship, this may lead to an infringement of people's right to freedom of expression (Art 19 UDHR, Art 19 ICCPR, Art 10 ECHR, Art 11 CFR, Art 13 CRC) and access to information, and also to a violation of their right to liberty and security of the person (Art 3 UDHR, Art 9 (1) ICCPR, Art 5 (1) ECHR, Art 6 CFR, Art 37 (b) CRC) if they are subsequently prosecuted for circulating content the government does not approve.

IV.4 CHILDREN'S INTERACTION WITH THE PRODUCT

ANALYSIS

The SASHA product has been designed with the intention that adult users can use it as an avenue to safely share images, including sexual images, while protecting their images from unwanted onward sharing. However, **children globally also share sexual images of themselves, commonly referred to as 'sexting'.** When done by teenagers, 'sexting' is a normal stage of child development by many experts. **However, in many jurisdictions, including in some countries in Europe, 'sexting' is criminalised as it is deemed to be self-production of child sexual abuse materials.**

- This means that if children use the SASHA app, it could produce evidence that may be used against the child in criminal proceedings. Children may be incentivised to use the App because it promises the 'safe sharing' of intimate images, which implies that their images will be kept private and that children will be safe from criminalisation.

- SASHA currently does not require any kind of age assurance steps such as asking the user for their age or date of birth or requesting proof that they are over 18. Some countries such as the UK require age assurance methods to be deployed by law on any site or app that contains a high risk to children. Age assurance has also been considered a mandatory requirement by the European Data Protection Board as a part of safety-by-design measures.

- Asking users to self-declare their age, or simply stating in the terms and conditions that children are not permitted to use the product would not satisfy these legal requirements. Age assurance is an extremely complex and rapidly evolving area because many of the age assurance tools on the market vary in their accuracy and accessibility, especially when it comes to minority groups, and may also introduce serious data protection and privacy risks. It is beyond the scope of this HRIA to fully interrogate all age assurance methods that could be appropriate for SASHA.

HUMAN RIGHTS IMPACTS

- Where children's intimate images are used against them in a criminal case this may violate their rights to privacy (Article 16 CRC), and to freedom of expression (Article 13 CRC).

- Furthermore, if age assurance tools are used to verify that children are not able to access the SASHA app, this may violate the right to privacy of both children and adults (Art 12 UDHR, Art 17 ICCPR, Art 16 CRC, Art 8 ECHR, Art 7 CFR) depending on the kind of age assurance tool used.

IV.5 ACCESS TO JUSTICE

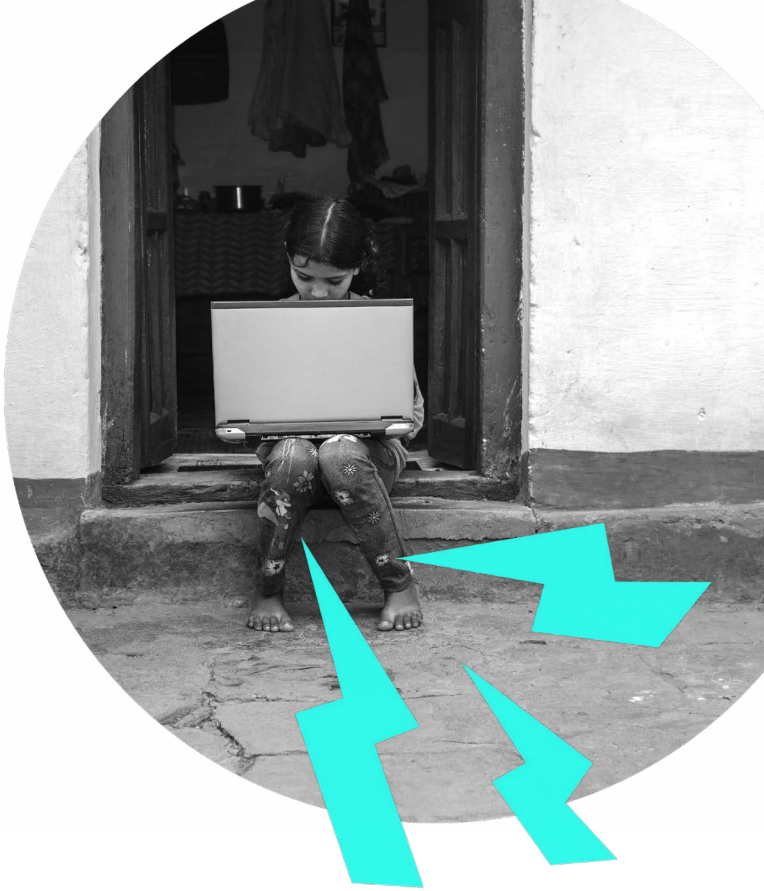
ANALYSIS

SASHA aims to empower victim-survivors to take back control and hold perpetrators accountable. There are many different scenarios that can result in a person becoming a victim-survivor of IBA or identity theft:

- A typical scenario involves a victim-survivor taking sexual images of themselves and sharing them with another person who then leaks these images against the will of the victim-survivor and often without their knowledge.

- In other cases, the perpetrator might secretly take images of the victim-survivor, either in a private setting (e.g. secretly filming sexual activity) or in a public space (e.g. a public toilet).

- Perpetrators might use generative Artificial Intelligence (AI) to create sexual images of the victim-survivor and share these with third parties.



- In cases of impersonation, a perpetrator might copy the image of the victim-survivor's social media account or secretly take a picture of them in private or in public.

All the above scenarios have in common that they lead to the victimisation of the person in the picture. However, **it is important to note that SASHA only protects the person who claims to hold copyright to an image, i.e. the person who is the original creator of the image in question. This is the person who took the image, not necessarily the person who is depicted in the image.** This means that the SASHA product only assists the victim-survivor who took the image themselves, i.e. who holds copyright. Further, the association of IBA with copyright could create the

impression that the harm experienced by victim-survivors is largely a violation of their intellectual property, rather than a violation of their privacy and human dignity. The conceptualisation of IBA as a copyright issue could hence mask the true nature of IBA, which is a form of sexualised, gender-based violence at its core.

In addition, SASHA aims to prove ownership and trace the non-consensual sharing of images back to the original source, thereby relieving the burden of proof on the victim. **When a victim-survivor is informed that their image has been shared without their permission, SASHA provides an 'evidence package' which might be helpful for victim-survivors who hold copyright of the image, i.e. who took the images themselves on their own phone.** Even in this case, SASHA can only prove that a person claimed copyright, not that the person actually holds copyright as SASHA does not require any proof that the person claiming the image is indeed the copyright holder. This risk is arguably minimised if the technology is integrated on device level, see B2B2C model.

IMPACTS

It is important to note that the above issues are a consequence of SASHA's business decision to focus on a specific group of victim-survivors. While it is commendable that SASHA is aiming to solve one significant part of the IBA landscape, and indeed it may not be possible to solve the entire IBA problem in one shot, we would like to flag the concerns raised during our stakeholder consultations with NGOs working with victim-survivor communities.

- Victim-survivors of IBA and identity theft experience violations of their dignity and privacy. SASHA needs to be careful not to provide hope about the effectiveness of its product to *all* victim-survivors, some of whom may not fall within the SASHA use cases (i.e. those who do not hold copyright of the images). Otherwise, victim-survivors who fall outside of the scope of SASHA may rely on the service to try to remove non-consensually shared images and restore their privacy which could make them feel misled.

- This might be further exacerbated as victim-survivors of identity theft or image-based abuse are in a particularly vulnerable position. Victim-survivors entrust the company with their sensitive information. Failure to provide an effective solution can result in a significant breach of trust and may deter others from seeking help. It is therefore important that SASHA's communications are clear regarding which kinds of IBA their product can help with and which it cannot.

Even where victim-survivors are given a package of evidence to take to a lawyer, access to justice in IBA cases is extremely challenging in most parts of the world, and most victim-survivors who do not have funds to pay a lawyer privately will struggle to make use of their evidence package and to access justice without legal assistance.

IV.6 RESPONSIBLE AI

ANALYSIS

SASHA is using AI to train its technology to identify non-consensually shared images. There are various human rights risks associated with the design, development, deployment and use of the SASHA technology from the perspective of responsible AI. **Considering that the product is in its early development stages, SASHA is only at the beginning of many of the processes and standards relevant for developing a responsible AI system.**

- Firstly, SASHA must ensure the fairness of its AI system, i.e. ensuring that datasets used for training the AI system are given careful consideration to avoid discrimination. T
he dataset needs to be diverse and relevant. If data from an open-source data base is used, SASHA needs to ensure that this data has been lawfully obtained (e.g. without copyright violations, or privacy violations regarding the depicted persons).

- Further, the robustness of the AI system must be a key consideration during the development and deployment stage of the SASHA product. Accuracy assessments should be repeated regularly throughout the different development stages and broken down into relevant metrics such as true negative, false negative, true positives and false positives. The false negative and false positive rates are particularly important to assess potential adverse human rights impacts, such as the effectiveness of the system to detect illegal content (false negatives) but also its potential to excessively block legitimate content (false positives).

- Transparency about the functioning of the AI system also needs to be a priority to ensure users understand how they

might be impacted by the use of AI within the SASHA product. Other aspects of a responsible AI system, such as non-maleficence and privacy, have been addressed in other sections.

HUMAN RIGHTS IMPACTS

Non-adherence to responsible AI standards such as human agency and oversight, technical robustness and safety, privacy and data governance, transparency and explainability, diversity, non-discrimination and fairness, societal and environmental wellbeing and accountability can have multiple adverse human rights impacts.

- The SASHA technology could potentially discriminate against people on the basis of different protected grounds, such as sex, race, ethnic origin, disability, age or others (Art 2 UDHR, Art 2(1) ICCPR, Art 14 ECHR, Art 21 CFR, Art 2 CRC, CEDAW, CRPD, ICERD), if the training data is not sufficiently representative of all users.

- Further, the SASHA technology could potentially infringe on the right to privacy (Art 12 UDHR, Art 17 ICCPR, Art 16 CRC, Art 8 ECHR, Art 7 CFR) of people interacting with the system, in particular with regards to their personal data, if their data is collected, stored and processed unlawfully.

- Further, the SASHA technology might adversely impact the right to privacy (Art 12 UDHR, Art 17 ICCPR, Art 16 CRC, Art 8 ECHR, Art 7 CFR) of the people depicted in the training data, if their consent for their images to be used in the dataset was not lawfully obtained.

- If the SASHA technology leads to false positives, this might further impact the right to liberty and security of the person (Art 3 UDHR, Art 9 (1) ICCPR, Art 5 (1) ECHR, Art 6 CFR, Art 37 (b) CRC) if persons are wrongfully accused of IBA or identity theft.

RECOMMENDATIONS

GOVERNANCE OF SASHA

- **Recommendation 1:**

Make the SASHA board of directors more diverse and equipped with human rights expertise

SASHA currently has a board of directors consisting of three men who are all also company investors. Therefore, SASHA should consider appointing board members from diverse genders and backgrounds, and a board member with expertise in human rights. This will assist the board to set strategic goals which respond to the lived reality of different populations, and which are in line with international human rights law.

- **Recommendation 2:**

Establish an independent advisory board

It is understood that SASHA intends to also establish an independent advisory board to leverage diverse expertise, industry insights, and networks to guide SASHA's growth trajectory and strategic decision making. This advisory board is planned to consist of technology innovators, legal experts, NGO representatives, ethical and social impact advisors, and strategic partners and investors.

As SASHA develops its independent advisory board it will be necessary to define clear objectives for the board regarding oversight over SASHA's product development and approach to human rights impacts as they arise. SASHA should define the advisory board's decision-making powers, and reporting requirements, as well as a clear process for SASHA to respond to reports prepared by the advisory board.

- **Recommendation 3:**

Embed human rights due diligence into SASHA's corporate governance structure

SASHA should create and publish a company policy commitment to respect and uphold human rights, with clear lines of accountability for its implementation. Further, SASHA should engage in ongoing human rights due diligence, including periodic consultations with external stakeholders.

SASHA should require named C-Suite staff to report to the board annually against clear goals related to human rights impacts and ethical decision making. These goals should be linked to staff key performance indicators.

THEMATIC RECOMMENDATIONS

POSITIONING IMAGE ABUSE AS A COPYRIGHT ISSUE

- **Recommendation 4:**

Do not overpromise victim-survivors to solve all IBA cases

It is important that SASHA does not overpromise victim-survivors to solve all their IBA cases. SASHA has the potential to play an important role to ensure victim-survivors have their images removed and seek justice. However, IBA is a complex, nuanced issue, and there might be many circumstances outside of SASHA's control which might lead to removal requests being unsuccessful. As an example, notice and takedown

requests are typically unsuccessful if the image is hosted on a website located outside the US or EU, and which has been set up for the sole purpose of IBA. These websites are highly unlikely to be interested in partnering with SASHA, and even if SASHA helps victim-survivors with an evidence package, these websites will likely simply not respond. From a victim-survivor perspective, it is therefore important that SASHA does not create expectations which it cannot live up to, as this could have detrimental impacts on victim-survivors who might see SASHA as their last avenue for help.

- **Recommendation 5:**
Work with the existing ecosystem to complement the efforts of other stakeholders

IBA is a complex societal issue which requires a multi-stakeholder approach to strengthen prevention and response efforts, which includes governments, NGOs, private sector, academia, and the general public. SASHA should continue to work closely with the existing ecosystem to ensure that their product complements and aligns with the existing efforts undertaken by other stakeholders. It could strengthen SASHA's relationship with NGO partners if it formalises these relationships through an independent expert advisory board (see recommendation 2) which has clear roles and responsibilities.

DATA PROTECTION

- **Recommendation 6:**
Complete a data protection impact assessment (DPIA)

SASHA should carry out a self-assessment of their data protection processes and practices and publish a data protection impact assessment (DPIA). There are guidelines available for this from the European Commission and further guidance is provided by the Danish Data Protection Regulator Datatilsynet. A DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. The findings from the DPIA should be used to inform the development of a comprehensive data governance framework, see recommendation 7.

- **Recommendation 7:**
Establish a comprehensive data governance framework

Based on the findings from the DPIA, SASHA should establish a comprehensive data governance framework with clear policies, procedures, and accountability measures to prevent unauthorised access or misuse of user data. For this purpose, SASHA should centre data minimisation and privacy-by-design principles in its product development process, only collecting and processing the minimum data necessary to provide SASHA's services. Further, SASHA should undergo regular third-party audits and obtain relevant data protection and security certifications (e.g., Europrivacy, ISO 27001, SOC 2) to demonstrate compliance with industry best practices. Lastly, SASHA should provide clear, transparent information to users about SASHA's data handling practices and give users meaningful control over their personal data, including the ability to access, update, rectify and delete it. SASHA should also include a mechanism to respond in a timely manner to any user requests about their data handling practices.

- **Recommendation 8:**
Implement comprehensive data security controls

SASHA should implement comprehensive data security controls, including end-to-end encryption, access management, and logging/monitoring, in line with industry standards such as ISO 27001 and NIST SP 800-171. Further, SASHA should develop and regularly test incident response and breach notification protocols to quickly address and mitigate any security incidents. SASHA should also undergo regular third-party audits and obtain relevant data protection and security certifications (e.g., ISO 27001, SOC 2) to demonstrate compliance with industry best practices.

PRIVACY

- **Recommendation 9:**
Commit to the protection of private communications

In the B2B2C model, SASHA aims to integrate its technology on platform level so the platform can scan all uploaded images against SASHA's database. While the scanning of content which is publicly available can be permissible under existing laws, private communications enjoy a higher level of protection under international human rights law and many regional and national laws. As SASHA centres the importance of privacy protection in its business model, SASHA should commit to the protection of private communications and

10

not deploy its technology when there is a risk that it will be used for general and indiscriminate scanning of private communications. This is particularly important when such scanning is targeting end-to-end-encrypted communications, as this might lead to the scanning of the content on device level (so called client-side scanning).

USE OF THE PRODUCT IN MORE AUTHORITARIAN COUNTRIES

The SASHA leadership team strongly emphasise that their personal and company values support anonymity and freedom of expression, and they do not condone or support censorship or repression. However, depending on where the technology is deployed, and how it is deployed SASHA might have to respond to government requests even if this does not align with their mission.

- **Recommendation 10:**
Explore joining the GNI Network and follow the GNI principles

Because this HRIA identifies high human rights risks for SASHA related to privacy and freedom of expression, it is recommended that SASHA considers joining the Global Network Initiative (GNI) Network, where they can obtain peer support and guidance on compliance with international human rights norms. The GNI Network provides a safe space for tech companies to assess their own policies and practices according the globally recognised GNI Principles on Freedom of Expression and Privacy, and to benefit from peer support from other tech companies as well as expert advice from academics and civil society. In line with the GNI Principles, SASHA should create a clear policy and procedure setting out how the company will assess and respond to government demands for access to data, or disclosure of personal information.

- **Recommendation 11:**
Include licensing requirements when selling SASHA to platforms

SASHA should also consider including contractual licensing requirements when selling its product to platforms. These requirements should bind platforms using the SASHA technology to respect due process and the rights to freedom of expression and privacy, so that the criteria of legality, legitimate aims, necessity and proportionality are applied when assessing government requests for access to data, in line with international human rights standards.

CHILDREN'S INTERACTION WITH THE PRODUCT

- **Recommendation 12:**
Determine measures to prevent children's access to the SASHA App

At present, SASHA's published terms and conditions foresee children accessing and using the App providing parental consent is granted and the child is supervised whilst using the product. The terms and conditions do not prohibit sexually explicit or pornographic material but do prohibit contributions that violate any applicable law concerning 'child pornography' or laws otherwise intended to protect the health or well-being of minors. As it is clearly foreseeable both that children will access the SASHA app, and that SASHA will be used for intimate image sharing, the product will be subject to specific legal risk and safety regimes.

SASHA should carefully consider the use of an age assurance tool. SASHA should ideally implement state of the art age assurance tools that are the most privacy preserving proportionate to the risk posed by SASHA to children using the app. However, it may be very difficult for SASHA to both have a high degree of certainty that it does not have any child users and offer a high degree of privacy to its adult users.

For further guidance on implementing the UNGPs in the digital environment through a child rights lens see the UN Human Rights B-Tech Project, Taking a Child-Rights Based Approach to Implementing the UNGPs in the Digital Environment: A B-Tech Special Briefing, 2024. (Tech Legality's co-founder Emma Day was one of the authors of this special briefing.)

ACCESS TO JUSTICE AND CONFLICT RESOLUTION

- **Recommendation 13:**
Centre a 'do no harm' approach in SASHA's access to justice interventions

SASHA aims to assist victim-survivors of IBA and identity theft to seek justice through various legal avenues. For this purpose, SASHA needs to centre a 'do no harm' approach in its access to justice approach. As an example, SASHA aims to give platforms the option to create a notification system which informs victim-survivors every time their image is being shared. Such a system might create considerable psychological distress for a victim-survivor, as every time the picture is shared it might bring back the traumatic experience.

Therefore, victim-survivors should be able to switch-off these notifications or choose how often they get notified (e.g. a summary report of monthly notifications, instead of instant notifications).

Further, SASHA should conduct a feasibility study about the needs of victim-survivors in the legal system under different jurisdictions to gain a better understanding what kind of supportive evidence SASHA can offer victim-survivors. Such a study would ensure that the evidence package provided for by SASHA is indeed useful for victim-survivors when seeking justice, tailored to their own jurisdiction, considering the known difficulties in accessing justice around the world.

- **Recommendation 14:**
Establish a company grievance mechanism to allow SASHA users to seek a remedy from SASHA where necessary

SASHA would also need a grievance mechanism for enabling individuals to report misuse of the App to SASHA, for example in circumstances where a user is bombarded with pornographic or other content via the App, or the App is used to falsely report the individual or other breaches of terms and conditions. While it is understood that the nature of the grievance mechanism in the context of the B2B2C model will depend largely on the platform it is integrated with, it is recommended that clarity around this is prioritised as soon as possible.

The UNGPs provide that for a company grievance mechanism to be effective it should be legitimate, accessible, predictable and equitable. See further UN Human Rights B-Tech Project, Designing and Implementing Effective Company-Based Grievance Mechanisms.

RESPONSIBLE AI

SASHA should commit to responsible AI principles which include developing, deploying and using AI systems in a way such that they respect the principles of respect for human autonomy, prevention of harm, fairness and explicability[2].

- **Recommendation 15: Conduct a self-assessment on SASHA's current status quo with regards to responsible AI processes and safeguards**

Conducting a self-assessment on SASHA's current status quo with regards to responsible AI processes and safeguards will assist SASHA to understand what risks an AI system might generate, and how to minimise those risks while maximising the benefits. As an example, SASHA could use the EU Commission High Level Expert Group on AI - Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment, which assesses whether the AI system that is being developed, deployed, procured or used, adheres to the seven requirements of trustworthy artificial intelligence (AI), including human agency and oversight; technical robustness and safety; privacy and data governance; transparency and explainability; diversity, non-discrimination and fairness; societal and environmental well-being; and accountability.

Based on the initial self-assessment, SASHA could develop a company AI ethics code, which sets out a clear purpose and scope, the principles SASHA commits to adhere to, and clear provisions around governance, implementation and monitoring of the AI ethics code. This code could be incorporated into the governance policies.

- **Recommendation 16:**
Test the SASHA product in a regulatory sandbox

SASHA should consider testing the SASHA product in an AI regulatory sandbox, such as the one established by the Danish data protection authority (Datatilsynet). A regulatory sandbox allows businesses to test their products under the supervision of the regulator which helps to better understand the regulatory landscape around AI development and deployment and how to implement responsible AI principles throughout the technology's design, building them into AI solutions from the ground up.

2 HLEG, Ethics Guidelines for Trustworthy AI, 2019.