Apple’s Conundrum

A Privacy Impact Assessment on Apple’s new child safety features

Umi Sonoda

10/12/21

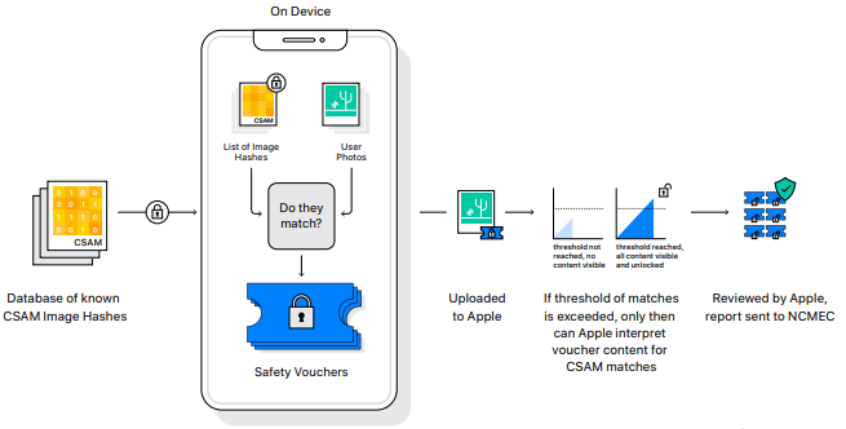
Background

On the 5th of August 2021, Apple announced three new "Child Safety" initiatives to tackle the spread of Child Sexual Abuse Material (CSAM) and predators using communication tools to recruit and exploit children. Key features of these data supply changes involved:

1. The 'Messages' app using on-device machine learning to warn Apple about sensitive content.
2. Its iOS and iPadOS using new applications of cryptography to detect the presence of CSAM in iCloud photos.
3. New Siri and Search updates intervening when users attempted to search for CSAM-related topics.

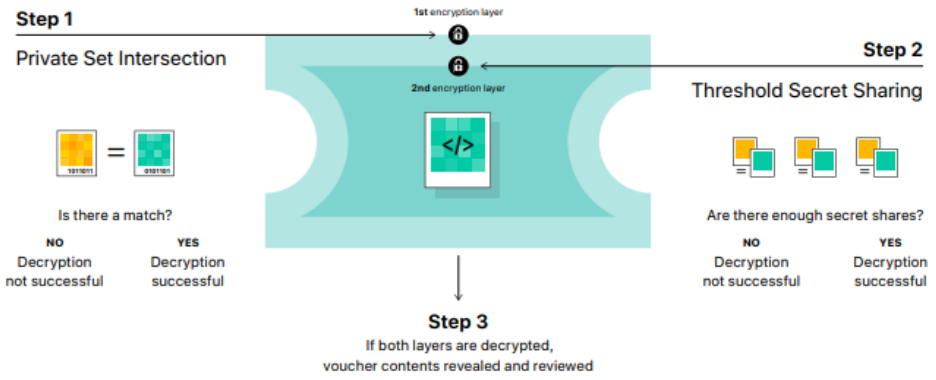
The data would be collected from Apple device users, image attachments stored in iCloud photos would be compared to known CSAM images from a third-party database, and flagged content would be shared and reported to the National Center for Missing and Exploited Children (NCMEC). The on-device data matching technology used in this process would help Apple to determine if there was a match without revealing the result. This prevented unnecessary data access to negatively-matching content and because these photos were not stored, it also removed the need to delete data. Included below, are diagrams depicting the data supply chain as well as its information flows.

Apple's On-device CSAM-matching Process



(Apple 2021)

Apple's Encryption Technology



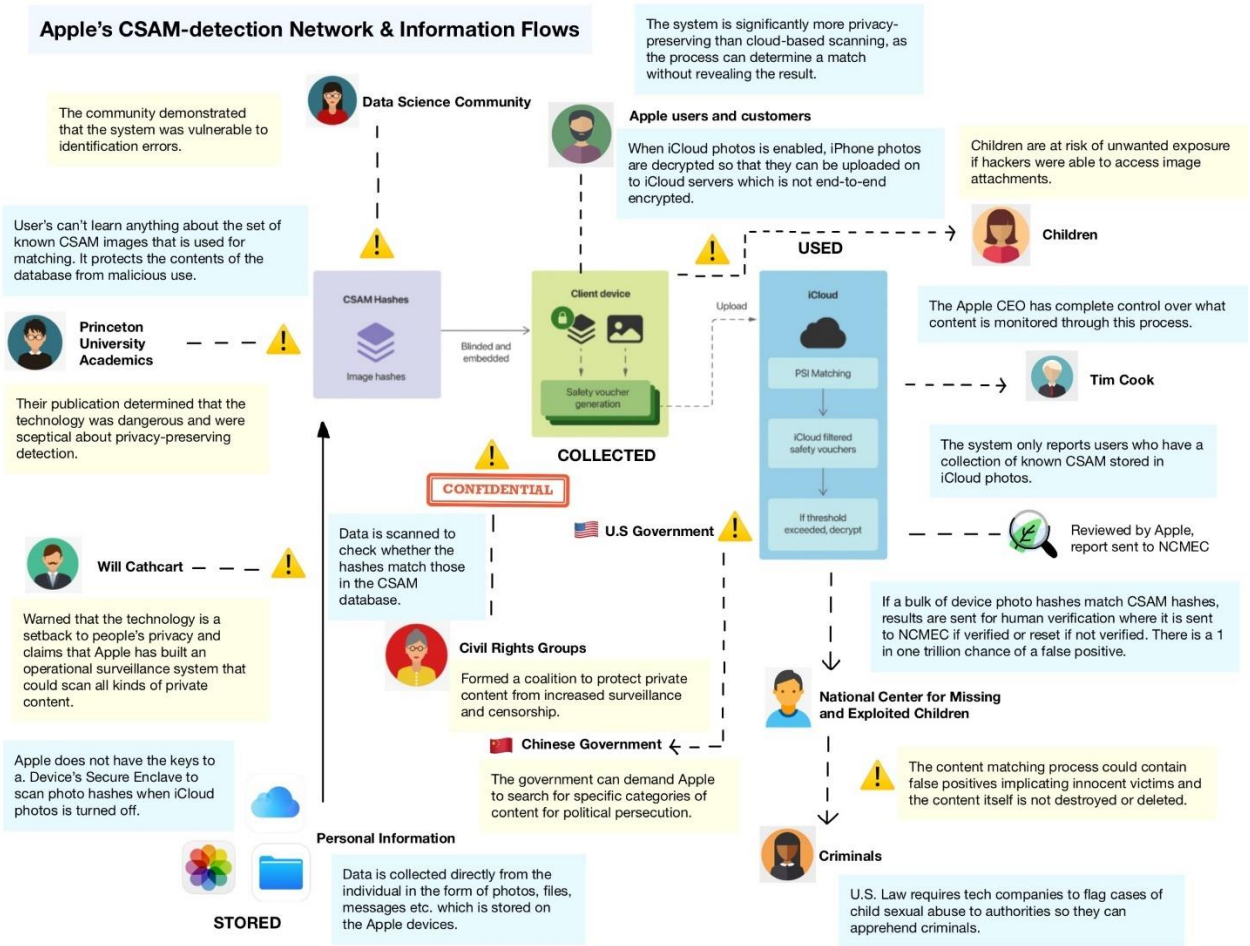
(Apple 2021)

As shown in the diagrams, two key data sources are Apple's multimedia devices and its cloud storage service, 'iCloud'. On the 28th of January 2020, there were 1.5 billion active Apple device users (Apple 2020) and since 2018, the iCloud service has had an estimated 850 million users (Novet 2018). The volume of data has only increased following this period and it encompasses a variety of information such as files, notes, mail, and messages, with a heavy focus on photos. The data itself is already highly sensitive in nature and because it is targeting explicit photos of minors, it requires careful consideration of the key stakeholders who could be affected (Appendix 1).

A Privacy Impact Assessment (PIA) is necessary because the data matching activities involve changes to Apple's existing information handling practices that would potentially affect all 1.5 billion users. There are also privacy implications associated with its usage and powerful institutions like governments, can extend its detection to other materials outside CSAM. Hence, privacy needs to be properly considered to create stakeholder trust and a willingness to adopt the new service.

Impacts

The following section will describe key privacy elements and their impacts if Apple were to implement the initiatives. The network map below depicts the extent and type of information that will be collected, how security and information quality will be addressed and how information will be used and disclosed.



Main Impacts

- **A backdoor for surveillance** – It rejects privacy as a social norm and portrays client-side scanning systems as something that needs to be accepted for the greater good of society.
- **Authoritarian rule and censorship** – It sets a starting point for powerful institutions to persecute pollical enemies. What stops the Chinese Government from demanding Apple scan devices for pro-democracy materials?
- **Third-party involvement** – Apple does not control the NCMEC database of illegal material because it is using on-device processing. Apple users will need to also trust that NCMEC handles their data appropriately, and this could include other third parties if they petition to add additional hashes specifying other material to the database.
- **Security risks** – Information could be easily exploited if the wrong group gained access to these database entries or even worse, obtained control.
- **Insecure communication** – Apple has access to all photos, messages, and notes as well as other content on a user's phone. The monitoring system will change the nature of private communication and give parents the power to control the social life of their children.

Unintended Impacts

- **Increased consumer costs** – From a computing resource perspective, it pushes the operational cost onto the user without compensation. Instead of Apple paying for their own servers to distribute the data, iPhones will become the distributed server system. Consequently, it would slow down the phone by using its CPU and wear it down over time, at the cost of the consumer.
- **Ambiguity around data ownership** – Whilst on-device processing is more favourable than decrypting photos on Apple's servers, it can raise further questions around who actually owns the device and the content on the device.
- **Psychographic profiling** – The hashes could be cross-checked against other databases from third parties containing unrelated material which determine political affiliation, sexual orientation, and other personal characteristics.
- **False positives** – Users will receive no direct feedback about whether their photos match the CSAM database and there is the possibility, although extremely unlikely, that innocent victims can be implicated. If this information was leaked it could cause irreversible damage to a user's reputation.

Ethical and Regulatory Concerns

Privacy Implications

- **Breaking secure end-to-end encryption** – The monitoring process is performed on the user's device which has the potential to bypass any end-to-end encryption (E2EE) that would otherwise safeguard the user's privacy. This leaves the door open to specific kinds of surveillance.
    - *Care ethics* – How do we ensure privacy for those under the age of 13? How do we prevent a slippery slope from occurring? (Bazerman & Tenbrunsel 2011)

    - *Deontological view* – How is the data from on-device processing going to be used? How is the data going to be stored?
- **Creating surveillance systems that operate on a user's device** – The infrastructure replacing E2EE is vulnerable to abuse and scope creep. New training data could be easily added to the algorithm for censorship purposes.
    - *Care ethics* – How can on-device processing be repurposed to expand human flourishing? How to reshape the technology for emancipatory ends?
    - *Deontological view* – How to rectify the power imbalance between organisations and users?
- **Trespassing privacy rights** – Apple is not necessarily accessing the device itself, but instead accessing the user's data that is on *their* device. They have intentionally exceeded the scope of authorisation to access a user's phone through client-side scanning.
    - *Care ethics* – How can the negative rights of multiple stakeholders be balanced?
    - *Deontological view* – How can users reclaim digital sovereignty? How can the negative rights of multiple stakeholders be balanced?

Issues of Public Concern

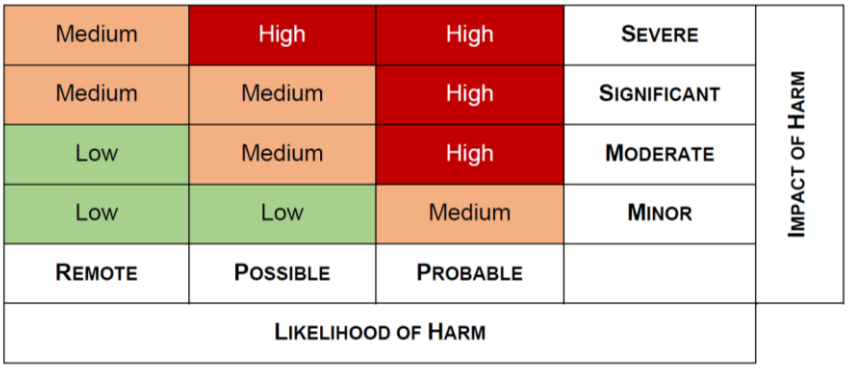
- The current end-user license agreement (EULA) or privacy policies that permit Apple to scan individual hard drives and iPhones for evidence of illegal misconduct (including CSAM) are vague. The company needs to be more explicit when asking for consent to access a consumer's files and data.
- There exists the threat of cryptographic attacks to reverse the encryption algorithm to recover encrypted data, and linkage attacks, using the encrypted data to identify people by linking the record with other known information.

Regulatory Considerations

- ***Computer Fraud and Abuse Act (CFAA)*** – What Apple plans to do is to scan the entire contents of every user's drive for CSAM or materials that are "inappropriate for minors". This raises a difficult question about what constitutes a "search" or an actionable search under the Fourth Amendment (Rasch 2021).
- ***Wiretap Law*** – There are questions around whether Apple is intentionally exceeding its authorisation to access user devices. Scanning for CSAM content does not constitute consent to the intercept of messages and FaceTime calls. What about the non-Apple user?
- ***Stored Communications Act*** – Online contracts imply that ongoing use of an Apple product means consent to the terms of the agreement, even after changes. It obfuscates what Apple can really do with the data.
- ***Title 18 of the United States Code Section 2252*** – There is the potential for felony indictment because Apple employees will need to identify CSAM on a user's device and then upload it to their own servers for manual review. This could violate U.S. law which prohibits knowingly transmitting, storing, and processing CSAM.

Risk Profile

The following table will be used to assess the identified risks and their harm to stakeholders.



Risk Assessment

Source of risk and impact	Likelihood of harm	Impact of harm	Overall risk
1. Collecting more information than is needed for future surveillance which introduces a backdoor that undermines the fundamental privacy protections of all users.	Possible	Severe	High
2. Using intrusive means of collection through on-device processing, impacting users' privacy and their ability to communicate privately.	Possible	Significant	Medium
3. Disclosing personal information more widely than is justified or necessary to other third-parties which decreases privacy for all iCloud photo users.	Remote	Significant	Medium
4. Information is saved onto personal storage devices, increasing the risk of accidental loss of personal information and exposure to cryptographic and linkage attacks.	Remote	Severe	Medium
5. Incorrectly identifying innocent users as criminals engaging in CSAM which would cause significant damage to the reputations of both the victim and Apple.	Remote	Severe	Medium
6. Collection notice will not be provided to all individuals who do not have the safety features enabled.	Remote	Moderate	Low
7. Changing stance towards encryption from end-to-end to on-device machine learning, which impacts the right to communicate privately.	Remote	Moderate	Low

Risk Mitigation Strategies

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
1. Surveillance and censorship	Apple has refused demands to deploy government-mandated changes to expand the technology to encompass other material. The detection	Reduced	Medium	Yes

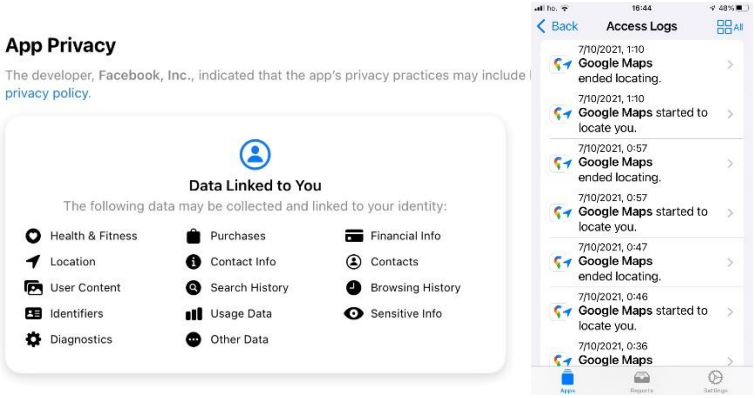
	capability is used for the sole purpose of identifying CSAM and nothing else.			
2. Invasive data collection	Functionality to opt-in or opt-out of iCloud photos - CSAM detection only applies to images that are uploaded to the iCloud photo library. Apple can only interpret the content when a certain threshold of matching CSAM images is exceeded.	Reduced	Low	Yes
3. Third-party disclosure	Apple has implemented data access restrictions to prevent access to non-CSAM images as well as utilising an encrypted database provided by two or more child safety organisations from separate foreign jurisdictions. Third-party data governance also increases privacy levels.	Reduced	Low	Yes
4. Security threats to personal information	Apple's technical and operational controls do not allow servers to decrypt any match data or to count the number of matches for any given account. It must first meet the threshold.	Reduced	Low	Yes
5. False positives	The cryptographic techniques have a probability of an image being falsely flagged at less than one in a trillion which is crypto-level negligible.	Reduced	Low	Yes
6. Notification of data collection	Increased communication strategies and an updated privacy policy mean that users know when the safety features are enabled and whether the system will send a notification (Appendix 3).	Accepted	Low	Yes
7. Encryption stance	The on-device processing occurs before sending and after receiving i.e., both endpoints, meaning that nothing changes about the E2EE inherent to Apple's messaging protocol.	Eliminated	Low	Yes

Recommendations

Accounting for proportionality and necessity (Appendix 2), Apple should implement the three new safety features in order to maintain a high level of user privacy whilst minimising false positives. Thus, the following is recommended:

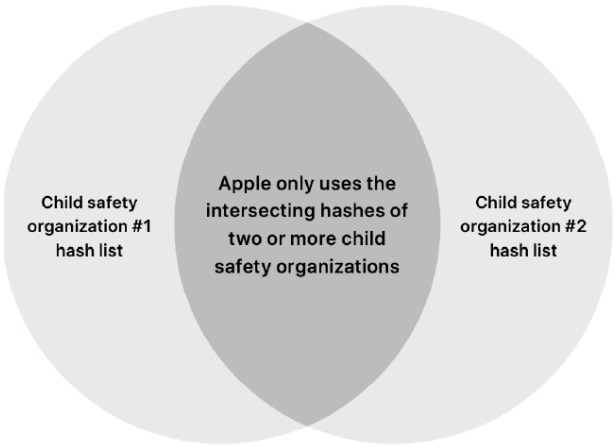
- **Privacy by design** – Apple must honour the original intentions of the system to detect CSAM, continue to refuse the government-mandated changes, and prevent its usage for other irrelevant material. This will mitigate the risk of surveillance and censorship.

- **Transparency measures** – Establish clear boundaries for data extraction and lay out rules of consent for an individual's privacy. Like the examples below, Apple should notify users of the data they collect, particularly when they collect it through access logs and issuing a warning notification if users wish to proceed. They should also keep the ability to opt-in and opt-out of using iCloud. This will reduce the risk of invasive data collection and poor notification.



(Apple 2021)

- **Flexible auditing** – Leverage the technical properties of the encryption system to guard against cyber-attacks and in turn rely upon the reviewers within Apple, to guard against the possibility of technical or human errors earlier in the system. In effect, this model will prevent errors occurring through automated and manual review. This will eliminate security threats and false positives.
- **Ethical code of conduct** – In addition to flexible auditing, Apple must ensure that they are not manufacturing consent for the 'greater good' or forcing users to blindly trust them, and respect that the personal information including the device content is owned by the user.
- **Compliance with regulations** – In the US, NCMEC is the only non-governmental organisation legally allowed to possess CSAM material. Apple generates on-device matching through an intersection of hashes provided by at least two child safety organisations operating in separate sovereign jurisdictions to comply with this law (Apple 2021). Additionally, transparency, consent, control, and confidentiality are design principles which have been incorporated by following the security and privacy requirements.



(Apple 2021)

References

Apple (2020). *Apple Reports Record First Quarter Results* [Press release]. 28 January. Available at: https://www.apple.com/newsroom/2020/01/apple-reports-record-first-quarter-results/ (Accessed: 4 September 2021).

Apple 2021, 'Expanded Protections for Children', *Apple*, 3 September, viewed 5 October 2021, <https://www.apple.com/child-safety/>.

Australian Institute of Criminology 2021, *Criminal justice responses to child sexual abuse material offending: A systematic review and evidence and gap map*, Australian Institute of Criminology, Canberra, viewed 9 October 2021, <https://www.aic.gov.au/sites/default/files/2021-03/ti623_criminal_justice_responses_to_csam_offending.pdf>.

Bazerman, M. & Tenbrunsel A. 2011, 'Ethical Breakdowns', *Harvard Business Review*, vol. 84, no. 9, pp. 1-9.

Bellare, M. 2021, *A Concrete-Security Analysis of the Apple PSI Protocol*, Department of Computer Science and Engineering University of California, San Diego, viewed 11 October 2021, <https://www.apple.com/child-safety/pdf/Alternative_Security_Proof_of_Apple_PSI_System_Mihir_Bellare.pdf>.

Bellare, M. 2021, *The Apple PSI Protocol*, Department of Computer Science and Engineering University of California, San Diego, viewed 11 October 2021, <https://www.apple.com/child-safety/pdf/Technical_Assessment_of_CSAM_Detection_Mihir_Bellare.pdf>.

Chuck, E. & Bailey, C. 2018, 'Apple CEO Tim Cook slams Facebook: Privacy 'is a human right, it's a civil liberty', *NBC News*, 28 March, viewed 8 October 2021, <https://www.nbcnews.com/news/amp/ncna860816>.

Duckett, C. 2021, 'Apple to tune CSAM system to keep one-in-a-trillion false positive deactivation threshold', *ZDNet*, 16 August, viewed 11 October 2021, <https://www.zdnet.com/article/apple-to-tune-csam-system-to-keep-one-in-a-trillion-false-positive-deactivation-threshold/>.

Electronic Frontier Foundation 2021, 'Apple Must Abandon Its Surveillance Plans', *Electronic Frontier Foundation*, viewed 7 October 2021, <https://www.eff.org/pages/apple-must-abandon-its-surveillance-plans>.

Feder, S. 2021, 'Apple has a new plan to curb child pornography. Here's why it's controversial.', *Popular Science*, 16 August, viewed 11 October 2021, <https://www.popsci.com/technology/apple-fights-to-limit-child-pornography-and-csam/>.

Forsyth, D. 2021, *Apple's CSAM detection technology*, Computer Science University of Illinois, Urbana-Champaign, viewed 11 October 2021, <https://www.apple.com/child-safety/pdf/Technical_Assessment_of_CSAM_Detection_David_Forsyth.pdf>.

Gruber, J. 2021, 'Apple's New 'Child Safety' Initiatives, and the Slippery Slope', *Daring Fireball*, 6 August, viewed 8 October 2021, <https://daringfireball.net/2021/08/apple_child_safety_initiatives_slippery_slope>.

Hardwick, T. 2021, 'EFF Pressures Apple to Completely Abandon Controversial Child Safety Features', *MacRumors*, 6 September, viewed 6 October 2021, <https://www.macrumors.com/2021/09/06/eff-urges-apple-abandon-csam-plans/>.

HT Tech 2021, 'Apple says 15% iCloud users don't have extra layer of security enabled for their data', *HT Media*, 11 January, viewed 4 October 2021, <https://tech.hindustantimes.com/tech/news/apple-says-85-of-icloud-users-have-an-extra-layer-of-security-for-their-data-71610371922386.html>.

Kelly, G. 2021, 'Researchers Label Apple's CSAM Detection System 'Dangerous'', *Forbes*, 24 August, viewed 8 October 2021, <https://www.forbes.com/sites/gordonkelly/2021/08/24/apple-iphone-warning-ios-15-csam-privacy-upggrade-ios-macos-ipados-security/?sh=7be910973456>.

Mayer, J. & Kulshrestha, A. 2021, 'Identifying Harmful Media in End-to-End Encrypted Communication: Efficient Private Membership Computation', *Security Symposium*, vol. 30, pp. 893-910.

McKinney, I. & Portnoy, E. 2021, 'Apple's Plan to "Think Different" About Encryption Opens a Backdoor to Your Private Life', *Electronic Frontier Foundation*, 5 August, viewed 9 October 2021, < https://www.eff.org/deeplinks/2021/08/apples-plan-think-different-about-encryption-opens-backdoor-your-private-life>.

Newton, C. 2021, 'Whatsapp CEO Will Cathcart on a rocky year for the app,' *The Verge*, 13 September, viewed 11 October 2021, <https://www.theverge.com/2021/9/13/22672756/whatsapp-ceo-will-cathcart-interview-2021-propublica-privacy-encryption>.

Novet, J. 2018, 'The case for Apple to sell a version of iCloud for work', *CNBC*, Sunday 11 February, viewed 4 September 2021, <https://www.cnbc.com/2018/02/11/apple-could-sell-icloud-for-the-enterprise-barclays-says.html>.

Office of the Australian Information Commissioner 2021, 'Guide to undertaking privacy impact assessments', *Australian Government*, 2 September, viewed 2 October 2021, <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>.

Panzarino, M. 'Interivew: Apple's head of Privacy details child abuse detection and Messages safety features', *TechCrunch*, 11 August, viewed 11 October 2021, <https://techcrunch.com/2021/08/10/interview-apples-head-of-privacy-details-child-abuse-detection-and-messages-safety-features/?tpcc=ECTW2020>.

Pinkas, B. 2021, *A Review of the Cryptography Behind the Apple PSI System*, academic review, Department of Computer Science Bar-Ilan University, viewed 10 October 2021, < https://www.apple.com/child-safety/pdf/Technical_Assessment_of_CSAM_Detection_Benny_Pinkas.pdf>.

Rasch, M. 2021, 'Is Apple's Client-Side Child Porn Scanning Legal?', *Security Boulevard*, 20 August, viewed 10 October 2021, <https://securityboulevard.com/2021/08/is-apples-client-side-child-porn-scanning-legal/>.

Robertson, A. 2021, 'Apple's controversial new child protection features explained', *The Verge*, 10 August, viewed 11 October 2021, <https://www.theverge.com/2021/8/10/22613225/apple-csam-scanning-messages-child-safety-features-privacy-controversy-explained>.

Whittaker, Z. 2021, 'Apple delays plan to roll out CSAM detection in iOS 15 after privacy backlash', *TechCrunch*, 3 September, viewed 8 October 2021, <https://techcrunch.com/2021/09/03/apple-csam-detection-delayed/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGtTLUrrdf39Q5TiOsZHda2Z-7TtbS_m6z6dDgVABC6VZ878B5oRlmbjkVTgYC5naauKixsQwqtLqfVJQfp5B-0bUvvBHlMGa3bJIiXLl_dCectCLgtbMCfOwec-XhJUmqH2YJI9JV8-ESAtvmDvByQBvJTLhuJpXEkBpnyIKLZi>.

Whittaker, Z. 2021, 'Apple's CSAM detection tech is under fire – again', *TechCrunch*, 19 August, viewed 8 October 2021, < https://techcrunch.com/2021/08/18/apples-csam-detection-tech-is-under-fire-again/>.

Appendix 1 – Key Stakeholders and Data Subjects

Key Stakeholders	Relationship	Vulnerabilities	Relative Power
Apple users and customers	iCloud, the Messages app, and Siri functionality is pre-installed into the operating systems of Apple devices. Thus, the information of all Apple users can be accessed at any time, and the only way to stop it is to knowingly disable access. *Control:* Users can control the photos in their iCloud account and hence what data is subject to CSAM detection.	The safety of users and their personal data are vulnerable to attacks from hackers. On-device processing may eventually lead to full end-to-end iCloud encryption which implies omnipresent surveillance.	The implementation of the technology gives Apple the power to engage in surveillance and censorship globally, provides ammunition to authoritarian governments looking to exert greater control over their citizens, and changes the meaning of secure communication between people. Apple will have the power to refuse and accept what content can be controlled through their devices and platforms.
Chinese Government	Apple closely collaborates with the Chinese Government and has agreed to move the personal data of its Chinese customers to the servers of a state-owned Chinese firm (Kelly 2021). *Control:* The Chinese Government has control over the entire Chinese population and potentially their data.	Foreign governments including the Chinese government may use the technology for surveillance of anti-regime activists, journalists, and political leaders from opposing nations. It leaves the citizens exposed to authoritarian rule, the chilling effect, and the fear of persecution.	Governments can manipulate the system by searching for specific categories of content with the user being none the wiser.
Civil Rights Groups (incl. The Electronic Frontier Foundation, American Civil Liberties Union, the Center for Democracy & Technology, Flight for Future etc.)	Close to 100 policy and rights groups demanded that Apple abandon its plan to rollout the new security features. These organisations created a petition and were able to acquire over 60,000 signatures from concerned users. *Control:* The Policy and Rights Groups are fighting for more control over their data.	The coalition protected the vulnerabilities of the everyday Apple user by demanding private content be protected from increased surveillance and censorship.	The combined power and activism of various organisations pressured Apple into delaying the implementation of the encryption technology. Their work demonstrated that multinational technological companies can still be held accountable, and the balance of power can still be rectified given enough support.
Criminals	Criminals spreading CSAM material and engaging in child exploitation with Apple devices and services would be identified and persecuted.	The content matching process could contain false positives implicating innocent victims.	CSAM victimisation is a form of trauma that has chronic impact on individuals due to the continued availability of materials.

	Control: Criminals will have no say about how their data is controlled because they do not want to be identified.	Malicious users could manipulate the system to subject naïve users to unnecessary scrutiny.	As access to the internet has grown, there has been a concomitant rise in CSAM offending.
Data Science Community	Ashuhariet Ygver reverse-engineered Apple's hashing algorithm into a script that was then published onto GitHub, a public forum and community with many data professionals. *Control:* The community will have some level of influence in the direction of how data is used and collected.	It allowed anyone to access the code and test the technology regardless of whether they had an Apple device or not, compromising the security of the technology. Hours after the code was published, a research scientist at Intel Labs discovered a hash collision, where two entirely different images produced the same hash. The false positives demonstrated that the system was vulnerable to identification errors.	Faults in an algorithm such as hash collisions, can be found by those in the data community. These observations have the power to make the cryptography systems used by technological companies redundant and they subsequently must be retired.
National Center for Missing and Exploited Children	NCMEC is a non-profit organisation that fights against child abduction, abuse, and exploitation. It also acts as a comprehensive reporting center for issues concerning the prevention and recovery from child victimisation. *Control:* From a legal perspective, NCMEC will have some control over the data if it matches with images in their own database and they wish to enact criminal justice.	There are a lack of common definitions and terminology across jurisdictions and research around CSAM material which makes it difficult to compile and record information. Detecting CSAM offending and countering it on Apple's products and services are complicated by evolution of the darknet and other encryption techniques (Australian Institute of Criminology 2021).	Fingerprint hash matching against NCMEC's database is already occurring in other major cloud hosting service and social networks. U.S. law requires technological companies to flag cases of CSAM to authorities. In 2010, Apple reported 265 cases, while Facebook reported 20.3 million and this is because of their decision not to scan for such material to respect privacy (Gruber 2021). However, they are aiming to obtain more surveillance power under the guise of sending information to NCMEC.
Princeton University Academics	Mayer and Kulshretha wrote a peer-review publication on how to build an automated system that detected harmful media and concluded that the technology was dangerous.	The academics were vulnerable to cognitive bias and university influence in determining the presentation of their information.	Academics have the power to objectively assess whether the encryption techniques meet the privacy requirements and technically feasible protocols. In this case, they were

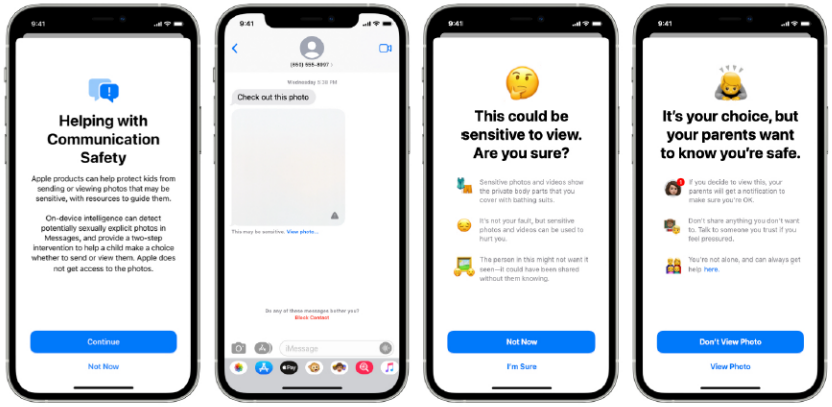
	Control: The academics will have some level of influence in the direction of how data is used and collected and assessing whether it is fit for purpose.	They identified the following vulnerabilities in the end-to-end encryption deployments: potential for abuse, false positives, attack surface, adverse externalities from international relations and market competition.	sceptical about privacy-preserving detection.
Tim Cook	The Apple CEO has been quoted saying that privacy is a human right and a civil liberty (Chuck & Bailey 2018). *Control:* Tim has complete control over the data that is readily shared by Apple users.	The German government asked the Apple CEO to reconsider the CSAM detection system, expressing concerns over its vulnerability to mass surveillance.	The CEO has the final decision around whether Apple should continue to implement the initiatives. In turn, he also has control over what content can be monitored as well as the level of privacy that users will have in the future.
U.S. Government	Apple provides customer data to the U.S. government almost 4,000 times in 2020 (Kelly 2021). *Control:* The U.S. Government has control over the entire Chinese population and potentially their data.	Apple may potentially be building infrastructure for surveillance which provide the U.S. government with the backdoor they need to monitor the vulnerable American population.	The government may obtain even more power if they can influence what content Apple controls by directing them to pinpoint political dissent and profile its citizens.
Will Cathcart	The head of Facebook's WhatsApp does not agree with Apple's unilateral approach and says it has built an operated surveillance system that could easily scan private content for anything they decide. *Control:* Will has complete control over the data that is readily shared by Facebook users and can challenge the how other companies view privacy.	Recent reporting showed the cost of vulnerabilities in iOS software and spyware companies have the potential to exploit this.	As an executive of a rival technological company, he has the power to hold similar organisations accountable. He also has the power to bring ethical considerations into more mainstream conversations.

Appendix 2 – Factors important to reducing or mitigating privacy risks

Factor	Definition
Necessity	Minimise the collection of personal information to what is strictly necessary.
Proportionality	Any negative privacy impact should be in proportion to, or balanced with, any benefits to be achieved from your project.
Transparency and Accountability	Privacy measures should be transparent to individuals, through adequate collection notices and privacy policies.
Implementation of privacy protections	Consider how organisational policies and procedures can support privacy, as well as practical elements such as staff training.
Flexibility	Take into account the diversity of individuals affected by the project, and whether they may respond or be affected differently to the sharing of their personal information.
Privacy by design	Privacy protections should be included in legislation or other binding obligations and built into new technologies from the beginning.
Privacy enhancing technologies	Consider whether any privacy enhancing technologies can be used in the project, and the impact of privacy invasive technologies.

(Office of the Australian Information Commissioner 2021)

Appendix 3 – Apple's communication safety in Messages



This new feature helps warn children and their parents when sending or receiving sexually explicit images.

(Apple 2021)